Master Thesis

A decision support framework for cybersecurity management

Jasper Hofman

Executive Master Cyber Security at Leiden University

1/22/2017

A decision support framework for cybersecurity management

by

Jasper Hofman

Student number 1727885

Executive Master Cyber Security

Leiden University

(Cyber Security Academy The Hague)

Acknowledgments

In these first lines of the thesis, I would like to take the opportunity to thank some people in particular. First, I would like to thank my family for their patience and support while I completed my Master study and wrote my thesis. I especially thank my wife.

This thesis would not have been possible without my employer and supervisor Henk van Steeg, who has given me the resources and freedom to free up much time to accomplish my Cyber Security Master course. I also thank my colleague Henk Schutte, who helped me to brainstorm on issues; the people who helped me to answer research questions during the interviews; and my graduation supervisors Jan van den Berg and Eric Luiijf, who critically reviewed the thesis and provided guidance to improve it further.

Abstract

"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." (Gartner, 2016). The aim of this research is managing organizational risk of cybersecurity threats in generic. IoT threats will be used as a starting point to explain the problem that organizations are facing concerning cybersecurity risk.

The IoT is a growing enterprise threat. For hackers, IoT systems are goldmines, as most devices are vulnerable by design because they are not built with cyber cybersecurity in mind cybersecurity. Cybersecurity risks arise as enterprises begin to deploy IoT devices for the business, and as employees bring those devices onto the corporate network. According to the Gartner Research and Advice Institute, more than half of major new business processes and systems will include an IoT component by 2020.

IoT risks are not stoppable if employees bring those devices onto the corporate networks. Installing IoT devices in the wrong place can create major incidents; therefore, organizations need to be resilient to these new threats by implementing suitable countermeasures. However, in practice several organizations are lagging behind in implementing cybersecurity countermeasures.

Almost everyone with digital experience knows or has heard of incidents such as viruses, ransom ware (lock of data files), and phishing emails from banks. Most of these incidents could be prevented if resilient countermeasures were implemented in a timely manner. For organizations, an incident can be a major risk; the impact can be financial, and board members including the CEO may need to step down as a consequence.

The goal of the research described in this thesis is *to develop an management decision support framework to safeguard businesses in a timely manner before (possibly high-impact) cybersecurity incidents become a reality*.

The methods used are scientific research into the literature, brainstorming, and interviews with cybersecurity experts with cybersecurity roles in med-size and enterprise organizations. The outcomes are used to develop the framework.

The results of the investigation show that cybersecurity risk is a strategic organizational risk because incidents can have a major impact on organizations. Moreover, many organizations do not deal with cybersecurity as a strategic risk, but at a low level within the organization, mostly within the Information Communications Technology (ICT) department. This means that strategic risk decisions are made without notice of the executive risk owner, and that Chief Information Security Officers (CISO) struggle with competing ICT projects and shared resources, which creates risky situations.

The developed framework helps executives to make decisions about strategic risk in an understandable way without cybersecurity knowledge, and to control or prevent key organizational risk from mitigation delays. The six-step framework supports the CISO to create shared stakeholder value throughout the organization by supporting effective cybersecurity risk reduction and needed project priority. The framework translates the cybersecurity threats into board-level controls. The framework is usable for cybersecurity in general and not only for IoT.

Further research possibilities could be the integration of other cybersecurity activities and projects – for example, the integration of audits, awareness, and repetitive tasks such as patching. In addition, specific framework aspects could also be integrated, such as ISF Standard of Good Practice maturity levels. The board would then be able to control cybersecurity processes based at desired maturity levels.

Table of Contents

1 Introduction

1.1 Dealing with the IoT cybersecurity risk

"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment." (Gartner, 2016). Recent developments in IoT technologies and the first set of IoT products have heightened the need for cybersecurity. Especially if enterprises integrate IoT into their Information Communications Technology (ICT) networks, risk management and cybersecurity measures are important to prevent incidents. IoT development is extremely relevant because of the often poor use of cybersecurity in organizations. Knowing the high risk of this type of innovation, the speed of organizational cybersecurity resilience (NCSC, 2015, p. 107) is especially important. IoT with its above mentioned cybersecurity risk has been the main reason for developing a management decision support framework to safeguard organizations against IoT risk and cybersecurity risk in general. From experience in various sectors and from discussions with Chief Information Security Officers (CISO), it is known that many organizations struggle to maintain resilience. There are many cybersecurity frameworks available for general governance, management, and best practice mitigation controls, but there is no practical guidance for handling cybersecurity projects within organizations at different organizational levels and between projects and stakeholders. Therefore, a management decision support framework will be helpful.

1.2 Practical relevance of the management decision support framework

The management decision support framework was developed with the aim to protect organizations from cyber incidents and as a response to CISO requirements for a practical improved guidance on cybersecurity project management for all projects. The framework has been based on best practices and several frameworks, as well as on the experiences of cybersecurity experts who have contributed, some with their mistakes or omissions, and others with their successes.

Project failures are all too common. Some make the headlines, especially with the cyber threats that organizations are facing. The reasons for failure are many and varied. Some common causes are:

- Insufficient attention to checking the organizational risk or business case
- Lack of communication with stakeholders and interested parties, leading to products being delivered that are not what the cybersecurity program executive wants
- Inadequate planning and coordination of resources, leading to poor scheduling
- Insufficient measurable key performance indicators and lack of control over progress, so that projects do not reveal their exact status until it is too late.

Without a cybersecurity decision support method or framework, those who commission a cybersecurity project, those who manage it, and those who work on it will have different ideas about how things should be organized and when the different aspects of the cybersecurity project will be completed. Those involved will not be clear about how much responsibility, authority, and accountability they have and, as a result, there will often be confusion surrounding the cybersecurity project. Without a cybersecurity program or decision support method, that takes the (cyber) "security by design principle" (CMMI, 2013, p. 3) into account, cybersecurity projects are rarely completed on time and within acceptable risk reduction, and this is especially true with other competing priority projects and budget constraints. A good cybersecurity project management method will guide the cybersecurity project through a controlled, well managed, visible set of activities to achieve the desired results (Fallis, 2013). The present management decision support framework adopts the principles of good practices to avoid the problems just identified, and thus helps to achieve successful cybersecurity projects or programs. These principles are:

- Cybersecurity projects and/or a program always need(s) to be managed in order to be successful;
- For genuine commitment to the cybersecurity project, all parties must be clear about why the cybersecurity project is needed, what it is intended to achieve, how the outcome is to be achieved, and what their responsibilities are in that achievement;
- Security by Design for improving organizational processes that lead to secure products and IoT implementations.

The benefits of using this management decision support framework are the following:

- The method is repeatable;
- The method is teachable;
- Building on experience;
- Ensuring that everyone knows what to expect, where, how, and when;
- Early warning of problems;
- Being proactive, not reactive, but also able to accommodate sudden, unexpected events.

1.3 Research question and objectives

The requirements needed to develop a decision support framework that can be used at all relevant organizational levels will be investigated, such as ICT departments and at the business and strategic board level. With this framework decisions can be made without proper knowledge of cybersecurity, and supports control of cybersecurity projects for timely implementation. This Thesis provides not only a theoretical framework, but also a practical guide to successfully govern the framework.

Implementing the framework can help to avoid unnecessary incidents due to the later implementation of key cybersecurity measures. The research goal is to develop an management decision support framework to safeguard businesses in a timely manner before (possibly high-impact) cybersecurity incidents become a reality. The findings should make an important contribution to the field of managing cybersecurity resilience within organizations.

The sub-questions that will be answered to reach the main goal are the following:

1) What is IoT?
2) Why is (IoT) cybersecurity important?
3) What is the organizational risk and potential business impact if (IoT) cybersecurity is not handled and prioritized as needed within organizations?
4) Are cybersecurity activities to counteract threats handled in a timely manner to reduce business impact?
5) What stops the organization from implementing countermeasures in a timely manner and what are the requirements needed to solve this issue?
6) Given the answers to the previous questions, how would a generic cybersecurity management decision support framework look like that also covers IoT for organizations?
7) Is the developed framework useful for large organizations?

Scope of the research

The following points fall outside of the scope of this thesis:

1) It will not cover how to implement IoT cybersecurity within organizations, or how to deliver an IoT cybersecurity measure framework to protect IoT systems or the organization itself.
2) It does not investigate whether organizations are already prepared for IoT adoption.
3) It does not investigate the effectiveness of IoT cybersecurity controls.

4) It only focuses on med- and enterprise-sized organizations.

1.4 Thesis overview

The thesis is structured as follows. The introduction consisted of the practical relevance and research questions. The following chapters presents the methodology, an explanation of the problem, and the impact of the given problem, literature review with regard to current best practices and frameworks. Based on the best practices, the literature review, and expert interviews, requirements are subsequently developed to build a decision support framework for management. The decision support framework is the result of the combination of requirements and best practices. The decision support framework is then tested on a practical case. Finally, the thesis ends with a conclusion.

2 Methodology

Different methods have been used to perform this research: literature review, research priorities within ICT departments, research the downside by a lack of control over cybersecurity projects, the importance of cybersecurity within organizations, as well as attending professional knowledge events to understand IoT. Interviews have been conducted to determine the business and societal impact and the current way of working regarding the prioritization of cybersecurity projects. A first-version solution framework has been developed using a combination of literature review and interview results. To test and improve the framework, a simulation case study has been executed to provide preliminary conclusions and advice recommendations. To reach a best-fit solution for different domains within the management framework, best practices within the subject fields have been used within the framework. The design science research methodology is used within this Thesis. Design science is fundamentally a problem solving paradigm. The goal of design science is utility to create innovations that define the ideas, practice, design and management that can be effectively and efficiently accomplished (Hevner, March, & Park, 2004).

To answer the research sub-questions, the following steps were taken:

1) Describe the relevant scientific literature that supports the subject goals;
2) Describe a real example case from which the research can be tested;
3) Conduct interviews with medium- and enterprise-sized organizations to analyze the research question and as input for possible solutions towards a framework; and
4) Perform and reflect on the analysis with the new framework illustrating the use and commenting on its strengths and weaknesses that influence competing priorities.

2.1 Design science

A specific design science framework from Hevner et al.(Hevner et al., 2004) was selected for this research. Design science creates and evaluates artifacts intended to solve identified organizational problems. The artifact creation relies on existing core theories that are applied, tested, modified, and extended through experience, creativity, intuition, and problem solving capabilities of the researcher.

- 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. (Hevner et al., 2004). In this research, the management decision support framework to safeguard businesses in a timely manner before (possibly high-impact) cybersecurity incidents become a reality satisfies the criteria of an artifact.
- Problem relevance. The objective of design science research is to develop technology-based solutions to important and relevant business problems. (Hevner et al., 2004). In this research, the research problem has been formed after the scientific literature research of current organizational problems in the cybersecurity field. Interest in the framework from the interviewees also proved importance and relevance of the study.
- Design evaluation. The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods. (Hevner et al., 2004). In this research, a nearly authentic fictive case study was used to evaluate the framework.
- 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. (Hevner et al., 2004). This research tries to fill the gap in the existing cybersecurity governance knowledge by introducing a novel framework.
- Research rigor. Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact. (Hevner et al., 2004). This research relies on proven Hevner et al.(Hevner et al., 2004) method in design science field in order to

develop a framework that considers organizational requirements (through interviews and brainstorm sessions) and existing recommendations (through literature research).

- 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. (Hevner et al., 2004). In this research, the design task involves the creation, utilization, and assessment of heuristic search strategies. The requirements and constrains are based on literature review of best practices and interviewees. The solution domain is tested through a fictive case study.
- Communication of research. Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences. (Hevner et al., 2004). Parts of the designed framework are built for technology-oriented audience by using cybersecurity best practices and for management-oriented audience by translating cybersecurity into organizational risk and business objectives.

2.2 Brainstorm sessions

To develop the decision support framework, brainstorming (ISO/IEC, 2009, p. 27) was done with a team of people within the cybersecurity expert field. It was an informal/formal process, like a group discussion. The brainstorming group consisted of four cybersecurity experts such as cybersecurity officers, cybersecurity specialists, and cybersecurity managers. These were senior experts with years of experience within cybersecurity, security, and ICT. Seniority was clear from their experience and background in different areas of business. The experts' have different backgrounds, operating in sectors such as defense, online retail, consultancy, and banking, dealing with strategic, tactical, and operational issues within their organizations.

As the facilitator, the first step was explaining the context of the given problem as described in chapter three, as well as the research question and the goal regarding the outcomes. The objective was to find key attention areas regarding the problem within organizations that need to be solved.

2.3 Interview structure

To make the link between the literature review, the best practices, and creating requirements for the new framework, multiple cybersecurity experts were interviewed. The interviewed experts were information cybersecurity experts, such as CISO and information cybersecurity officers working at med- and enterprise-sized organizations. Their organizations are located in several countries with different backgrounds and expertise, such as the industry, government, and commercial sectors. Semi-structured interviews were used so that the respondents could broaden or zoom in on topics of their own expertise. The interviews were based on pre-defined interview questions (Appendix A) and oral discussions.

Qualitative research was used to provide insight into the problem and to dive deeper into the problem. The interviews were held individual. The results of the interviews were processes in a logbook (Appendix C) to secure the validity of the outcomes.

For reasons of confidentiality and privacy, the organizations and respondents are not listed by name. The interviewees of the different organizations operated in the public-private and private sectors at the strategic and tactical levels within the field of cybersecurity.

3 On the need for safeguarding against IoT risk

Within this chapter IoT is used as an example for the need of safeguarding organizations from cybersecurity risk. The cybersecurity landscape is much broader than only IoT, but IoT is used as an example because it is a new organizational threat. IoT is a new innovative technique and is a fast growing innovation market within society and industry. With the introduction of this new technology also comes new risk that needs to be safeguarded against to protect organizations from potential risk or incidents. The IoT risk and why safeguarding – to "protect from harm or damage with an appropriate measure" (oxforddictionaries.com, 2016a) – is needed, will be described in this chapter. The chapter draws from other cybersecurity incidents than IoT because IoT is new and there are not many examples available with public high impact.

IoT

Within this section the research sub-question "What is IoT?" will be answered. There are many different definitions of IoT. Although the words "Internet of Things" suggest that the IoT components are always related to the Internet, this is not the case. Gartner's definition of technology is much broader: *"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."* (Gartner, 2016) IoT within the industry is named IIoT. Figure 1 shows an example of an IIoT system that interacts with a mobile application.

Figure 1. Example of IIoT (Belden, 2016b)

The general characteristics of the current IoT generation are as follows: IoT is built based on functionality, and cybersecurity is often omitted. IoT is a new development and still full of cybersecurity risk because of its vulnerabilities and weak design (Economist, Unit, & Enterprise, 2016). Implementing compliance with cybersecurity controls is even more important than without IoT if IoT is vulnerable by design. If an organization which uses IoT fails to comply with cybersecurity controls, this can result in major risk. Examples of IoT and IIoT solutions within med-size organizations and different sectors are as follows.

Industry. An industrial IoT pilot was started within a SmartFactoryKL production line. The IIoT component connects production modules into smart factories and provides fast data communication. (Belden, 2016a)

Electric Power. An example installation is a West Coast utility and a leading East Coast power organization in the Western United States. It connects legacy sub-stations to the smart grid using GarrettCom IIoT routers. The benefits are access to real-time data, automated remote monitoring, and

extending the life of existing assets by integrating them into a modern sub-station communication network (Belden, 2016).

Oil transport. A United States-based midstream oil organization monitors a remote pipeline using cellular IIoT connectivity solutions. The cellular IIoT network collects data from programmable logic controllers (PLCs) along the pipeline and quickly pinpoints line pressure issues and locates leaks. The result is improved pipeline integrity and safety (Belden, 2016).

Public Transport. A major metro rapid transit system operator in Spain has implemented a coach-to-trackside video-monitoring infrastructure based on IIoT. The benefits are improved operational and safety monitoring, with faster incident response time (Belden, 2016).

There are organizations such as Belden that have safeguarded the cybersecurity of their IIoT in the above examples, but in many commercial cases safeguarding is not common. A research by Hewlett Packard Enterprise, a worldwide multinational information technology organization, show that IoT systems are vulnerable and have weak designs (Hewlett Packard Enterprise, 2015). Using vulnerable IoT systems for business purposes means that that the IoT cybersecurity risk is hard to manage; this can result in a potential organizational disaster. A different approach is needed to mitigate these IoT risks to protect organizations from disaster. This thesis provides guidance in reducing the chance of a potential disaster by providing a decision support framework with links to IoT best practices for safeguarding IoT systems.

3.1 Importance of adequate (IoT) cybersecurity protection

Within this section the research sub-question "Why is (IoT) cybersecurity important?" will be answered. The importance of traditional ICT is a prime example of the importance of IoT cybersecurity protection. The main difference compared to IoT cybersecurity is the interconnectivity of the IoT system and the possible vulnerabilities and weak cybersecurity design of the product. The chance of being compromised due to these vulnerabilities is much higher for IoT. Today's enterprises rely on information systems to keep day-to-day operations running and delivering business functions. These information systems are increasingly connected or exposed to the Internet by innovations such as cloud services, and to cyber threats such as phishing emails in the corporate network. A cybersecurity compromise could result in severe disruption of business functions, operational processes, and damage to the brand and reputation or to customers. Cybersecurity continues to fight a war against cyber attackers, even as data breaches and cybersecurity compromises have become unfortunate realities of transacting in today's digitized economies. ICT cybersecurity is evolving to combat new threats, but nefarious actors are always seemingly one step ahead of the game.

The financial executive (FE) (Gregg, 2010) published an article titles "The CFO's role in managing cyber risk," which argues that most organizations do less than they should to manage the risk associated with their handling of sensitive information. The author quotes Richard Schaffer from The National Security Agency: *"Eighty percent of cyber risks were preventable using existing standards, practices and technologies."* (Gregg, 2010)

The key factors contributing to this growing problem are old approaches to management structure and accountability for risk that are not aligned with today's environment. Cyber threats are doubling each year, and business cases for cybersecurity remain a major challenge because management often does not understand either the scale of the threat or the requirements for the solution. The FE report notes that financial losses are increasingly occurring because most organizations do not take a holistic, enterprise-wide management approach to quantifying and addressing cyber risk. It is common to consider this problem as an "ICT issue" instead of an enterprise-wide one (Gregg, 2010).

In the Target Corporation hack case[1], the total estimated cost of the attack was approximately $300 million. As a result of the hacking of the American organization Target in 2014 and Wyndham Worldwide Hotels, the CEOs had to leave the organizations because the directors *"failed to take reasonable steps to maintain their customers, personal and financial information in a secure manner."*(Post, 2014) There are also other reasons for directors to be intimately involved with decisions concerning an organization's cybersecurity: the regulators. These include compliance, inspections, and examinations of the cybersecurity by authorities and law, such as general data protection regulation (Ferrillo, 2014).

The Institutional Shareholder Service (ISS) provider of corporate governance and responsible investment solutions has concluded that considering of Target's responsibility to its customers, the corporate directors and committees should have been aware of, and more closely monitoring, the possibility of theft of sensitive information. Cybersecurity is new for many directors, and is certainly far from intuitive. Organization directors must have the responsibility to oversee their organization's cybersecurity program (Ferrillo, 2014). The FE report and ISS example indicate that organizations are not always aware of the cybersecurity risk and necessary enterprise-wide approach to managing cybersecurity. The enterprise-wide cybersecurity approach for IoT is not much different than the cybersecurity approach, only the management of countermeasures for IoT is much different. IoT will be elaborated in the best practice landscape (Chapter four).

3.2 Predictive IoT problem growth

The question is whether IoT is really a problem for organizations. Will organizations adopt IoT? For most people, this is hard to imagine; therefore the best way to answer the question is to look at several research studies.

The IoT is new in today's society. Businesses are starting small and adopting new IoT technology for limited usage. According to Verizon, however, the worldwide use of IoT is increasing fast. The forecast is that today's businesses are building IoT into future strategies and business models for product sales. Organizations across all industries now have IoT squarely on their radar. The worldwide IoT market expenditure will grow from $591.7 billion in 2014 to $1.3 trillion in 2019, with a compound annual growth rate of 17%. The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019, hitting 30 billion in 2020 (Verizon, 2015).

According to a report by Business Insider Intelligence, IoT can be called the next industrial revolution (Greenough & Camhi, 2016). The report states that the expected growth is enormous and includes not only the civil sector, but also other sectors and industries.

Industry 4.0 stands for the fourth industrial revolution. Best understood as a new level of organization and control over the entire value chain of the life-cycle of products, it is geared towards increasingly individualized customer requirements. Industry 4.0 combines production methods with state-of-the-art ICT (platform4.0, 2016). Industry 4.0 is an example in which IIoT will become an important component. IoT will change the way in which all businesses, governments, and consumers interact with the physical world. While the benefits of IoT are great, the reality is that existing ICT infrastructure cybersecurity is not keeping up with the pace of innovation. As we increasingly integrate network connections into (critical) infrastructure, important processes that once were performed manually are now vulnerable to cyber threats due to this IoT integration. Our increasing dependence on network-connected technologies has grown faster than the means to secure these technologies (Homeland Security, 2016, p. 2). This prediction of growth and cross-sector integration

[1] Through the hack of an air conditioning and heating supplier, which captured target Virtual Private Network (VPN) credentials. Using targets VPN to gain access to the network and hack 1800 nationwide cash registers which exposed 40 million customer debit and credit card accounts.

indicates what the problem might be if organizations do not properly execute management of cyber cybersecurity within the organization.

3.3 Impact/Risk

This section elaborates on the business impact and risk. The research sub-question "What is the organizational risk and potential business impact if IoT cybersecurity is not handled and prioritized as needed within organizations?" will be answered. First, the definitions of risk and impact are provided to ensure a better view on the given problem. The definition of risk is the following: "The potential that a given threat will exploit the vulnerabilities of an asset, or group of assets, and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and the severity of its consequences" (DNS, 2015, p. 24) Impact is defined as follows: "Adverse change to the level of business objectives achieved" (ISO/IEC, 2013a)

IoT systems introduce risk that includes malicious actors manipulating the flow of information to and from network-connected devices, or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, and potential disruptions to critical infrastructure. The impact of IoT systems on the organization, as described in section 3.1 "Importance of adequate IoT cybersecurity protection," depends on the IoT function within the organization. What is important for organizations is to assess the risk of the implementation of IoT systems, and to implement applicable best-practice IoT countermeasures to safeguard the IoT system against organizational risk. The implementation of applicable best practice measures is related to the organizational risk.

IoT risk

What is IoT risk? HP states that the risk of IoT devices arises from weak cybersecurity in the designed IoT products. Analyzed IoT products from manufacturers of TVs, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales, and garage door openers. Six out of ten researched products provide user interfaces that contain vulnerabilities, such as cross-site scripting and weak credentials; 70% use unsecured network services; and 90% of these devices collect personal information to the cloud of mobile applications (Hewlett Packard Enterprise, 2015). According to HP, cybersecurity for IoT is not a one-time implementation; instead, it is important for the whole life-cycle of the product. Cybersecurity should be seen as a continuous process. To counter threats, software updates are highly important to maintain a robust and secure system (Hewlett Packard Enterprise, 2015). Within critical infrastructures, systems should last for a whole contract term or should be replaced.

Cyber-attacks crossing into the physical world of industrial systems mean that not only physical systems could go down. A sophisticated attack could also cross the line from cyber to the physical world resulting into actually costing human life. There have been no big cross-over IoT incidents yet, but the evidence and research are mounting that the risk of occurrence here is real. Already with normal ICT, there are multiple examples of incidents that resulted in loss of life coming from human or ICT errors in Industrial Control Systems (ICS): events such as a gasoline pipeline rupture in Bellingham, Washington; a fire in DC Metro; and the Northeast blackout. David Meltzer, member of the Information Systems Security Association, indicates that there are malicious actors actively exploiting ICS systems, and these same ICS environments have shown that the impact of events can cause the loss of human life (Castellote & Ph, 2015). Introducing IoT can even create risk that malicious actors succeed if IoT is not secured using available IoT cybersecurity best practices. Therefor IoT best practices must be included in the framework that is developed in this thesis.

Learning from the past

Previous sections have made it clear that there are many new threats associated with introducing IoT. However, there are not many examples of IoT incidents yet, especially not within organizations. The following two examples show the risk:

- IoT NEST Hack. At the Blackhat Hackers Conference, hackers showed how they used the IoT to hack the NEST thermostat. With the NEST thermostat, one can adjust one's home temperature from one's mobile device. The hackers showed how they manipulated the device and how they rerouted data to their own servers, including daily timestamps of home uses, leaving home, and Wi-Fi usernames and passwords (PCM & Hofmans, 2015).
- An IoT hacking attack led to widespread outage of popular websites. Internet-connected IoT devices such as digital home cameras were hacked through weak cybersecurity configuration and design. The thousands of IoT devices where misused to generate a 620Gbps distributed denial-of-service (DDoS) on KrebsOnSecurity.com, causing the site to go offline (KrebsOnSecurity.com, 2016).

These examples are not organization-use related; they did not impact the organizations using IoT themselves. However, they illustrate the vulnerability and risk of IoT. Next to the IoT examples, it is important to learn from previous events with traditional ICT. This section presents examples of incidents that had a big impact on business operations of organizations.

The following section answers the research sub-question "Are cybersecurity activities to counteract threats handled in a timely manner to reduce business impact?" by using literature research. Looking at worldwide cybersecurity incidents and my own experience within the field, organizations are compromised mostly due to a lag in patching, obsolete systems, bad architecture, or lagging in implementing the right cybersecurity measures. Within these organizations, cybersecurity is still immature. For example, in the 2014 Sony hack started with a phishing email: the perpetrators gained access to Sony's internal network by sending phishing emails to Sony employees. Malware was attached to these emails, which gave hackers access to Sony's internal network (SANS, 2015). As a result, senior officials' wages, films, employees' and celebrities' personal data, and confidential business information were captured. The damage resulting from the attack was also significant for Sony Pictures Entertainment's reputation. Sony estimated the direct damage of the cyber-attack to be worth $15 million (Hornyak, 2015). These were mainly research and remediation costs. Mark Rasch, a former federal cyber-crimes prosecutor, estimated that costs could run up to $70 million.

Why was this hack so successful within Sony? Did the organization not practice cybersecurity? Considering the used attack method, with the right cybersecurity measures this hack probably could have been stopped at an early stage. A case study called "Critical Controls that Sony Should Have Implemented" by SANS institute (SANS, 2015) confirms that this incident could have been prevented by implementing specific countermeasures. The following hack examples show impacts that could have been prevented if there had been correct cyber controls in place:

- Carbanak: In 2015, the Carbanak cyber-criminal gang stole up to $1 billion from financial institutions worldwide using targeted attack methods (Kaspersky, 2015) such as phishing emails.
- In April 2016, the German Gundremmingen nuclear power station in Bavaria was infected by malware through an infected USB-drive (security.nl, 2016b).
- German defense contractor Rheinmetall was infected by malware in 2016. According to Volkskrant sources, the attackers "certainly" obtained access to technological information from the organization and had control over the organization's network through social engineering and malware (security.nl, 2016a).

3.4 Competing priorities

Within this section the research sub-question "What stops the organization from implementing countermeasures in a timely manner?" will be answered by analyzing literature research. What are competing priorities? A priority is the fact or condition of being regarded or treated as more important than others (en.oxforddictionaries.com, 2016c), while to compete means to strive to gain or win something by defeating or establishing superiority over others (en.oxforddictionaries.com, 2016a). The competing priorities for cybersecurity are activities needed to accomplish a task. This can be cybersecurity projects or tasks.

In most organizations, cybersecurity is positioned within the ICT department. The controls to protect the organization from a risk are mostly technical and need to be implemented within the ICT department. Priority and project competitions play a role within this playing field because the ICT department has more objectives and business need than only cybersecurity.

Analyzing cybersecurity incidents reveals that they could mostly be prevented by taking cybersecurity seriously and implementing the best practices suitable to the organization. Regarding the Sony hack, the SANS institute published a case study showing that critical control could have stopped the attack at an early stage (SANS, 2015). In addition, from my own field experience as a cybersecurity expert, I have seen many organizations struggle with securing their environment. Shortly described, cybersecurity is mostly important for organizations, but it must not slow down the business. Other projects have more short-term priority, projects need more time to finalize, and the same resources are needed for cybersecurity projects as for other ICT projects. The ICT department has more goals and objectives than cybersecurity alone, and the two can even clash. Not every manager has the right capabilities to oversee the cybersecurity risk. If there is no dedicated team or if cybersecurity is not one of the organizational strategic objectives, the CISO has a heavy task between the competing priorities.

According to a study by Security of Things World USA (Security of Things world USA, 2016, p. 11), competing priorities is the top reason, next to lack of expertise and budget constraints, for blocking enhancements of current cybersecurity levels in organizations. These enhancements, including new protecting features, up-to-date systems, and vulnerabilities, are needed to protect organizations' interest. If organizations' blocking behavior regarding cybersecurity enhancement continues, this behavior will be a major issue for IoT adoption and organizational risk. The competitive priorities are a serious problem in preventing cyber risk for organizations. In addition, Richard Schaffer from the National Security Agency confirms that 80% of cyber risks are preventable using existing standards, practices, and technologies (Gregg, 2010). This thesis will provide a practical framework for supporting organizations with decisions regarding competing priorities to maintain cybersecurity.

3.5 Summary

The adoption of IoT is a matter of time. Businesses will be the top adopters, as well as governments focusing on increasing productivity and decreasing costs. The downside of IoT is immature integration of cybersecurity (no cybersecurity by design principle), and the controllability of its vulnerabilities. For organizations, this can be a serious problem with societal impact or financial loss if controls are not implemented in a timely manner.

Moreover, several sources have stated that cybersecurity could be prevented if the right cybersecurity measures had been implemented. To prevent business being impacted by cybersecurity attacks, it is important to implement risk management and the right mitigating controls. As was seen in the examples above, the problem is not that there is no way to protect the business, but more that these controls must be implemented in a timely manner. Based on the literature review, my own experience, and an explorative review, it seems that cybersecurity is often an ICT topic. Projects are managed

inside the ICT department and cybersecurity projects are overruled by competing priorities. The missing of countermeasures, the competition problem, incidents, and impact will feed the research and solution for the development of the decision support framework.

4 The best practices landscape

This chapter elaborates on the generic cybersecurity governance and IoT strategic, architecture and securing IoT best practices, as well as on the management of key activities or projects to safeguard the implementation of IoT countermeasures.

The problem description in Chapter three concerned the threats related to the cybersecurity posture of IoT and the problem of implementing cybersecurity-related countermeasures in a timely manner before the organization is exposed to organizational risk, with cybersecurity incidents as a result. Organizations' cyber governance focus must be on cybersecurity to implement countermeasures within the organization in a timely way, and on the practicality to control or steer the cybersecurity strategy and roadmap. This chapter investigates the current best practices for information security, such as ISO/IEC 27001/2 (ISO/IEC, 2013b), the Information Security Forum (ISF) Standards of Good Practice(ISF, 2013), NIST SP 800-53, and the Cyber Security Framework(NIST, 2014b). The chapter will examine whether the governance of a cybersecurity roadmap is covert, and whether these frameworks provide guidance to manage the implementation of the cybersecurity program. This chapter will also interpret the requirements specific to the cybersecurity implementation and management of IoT, because these new requirements are outside of the existing frameworks and are required for the cybersecurity of IoT implementations.

4.1 Cybersecurity governance within organizations

Figure 2. Governance levels

This section investigates the top three best practice frameworks for cybersecurity. To govern cybersecurity within an organization, many tested best practices or standards for traditional ICT cybersecurity can be applied to IoT. These best practices govern strategic, tactical, and operational layers, as shown in Figure 2, of cybersecurity within organizations. When researching best practices, it came across that literature mostly focuses on the above mentioned practices. Although more at the tactical and operational levels than on the strategic one, because the best practices are more guidelines and standards than governance alignment with business. These best practices concern the top-level policy, countermeasure frameworks, and standard and operational procedures to identify vulnerabilities. They are also used to set-up a process for incident response, and include procedures to recover from damage or disruptions. Three main example, best practice, standards to govern (cyber)security within the organization are the following:

- ISO/IEC 27000 series (ISO/IEC, 2013a). Leading cybersecurity standards and best practices include the International Organization for Standardization (ISO)'s information cybersecurity series. This is also known as the Information Security Management System (ISMS) family of standards. The series provides best practice recommendations on information cybersecurity management, risk, and controls.

- NIST Special Publication 800-53Ar4 (NIST, 2014b) and Cybersecurity Framework (NIST, 2014a). This covers the steps in the Risk Management Framework that address cybersecurity control selection for federal information systems in accordance with the cybersecurity requirements in the Federal Information Processing Standard. The Cybersecurity Framework (NIST CSF) provides a policy framework of computer cybersecurity guidance regarding how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It provides high-level taxonomy of cybersecurity outcome and a methodology to assess and manage those outcomes. A new 2017 draft version of the Cybersecurity Framework is published. The main changes are: new section measuring and demonstrating cybersecurity, cyber supply chain risk management, refinement section access control and establishing or improving a cybersecurity program.
- Information Security Forum (ISF) (ISF, 2013). This delivers the standard of good practices for information cybersecurity and is available to ISF members. The standard is a business-focused, practical, and comprehensive guide available for identifying and managing information cybersecurity risk within organizations.
- NIST Special Publication 800-160 Systems Security Engineering. (NIST, 2016b) Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. This publication addresses IoT engineering based solutions, the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems.

Reviewing these best practice frameworks for governance and IoT, is clearly focused on setting policy, and implementing the right measures and procedures to govern cybersecurity within organizations. The best practice that best fits into the internal processes and culture is an organization-specific issue. Because of the diversity of organizations and their businesses, the best method is to use one framework combined with topics from other frameworks. Figure 2 shows the different organizational levels of the frameworks. The ISO/IEC 27001/2 series is a governance framework to govern cybersecurity through the whole organization using policy and processes at the tactical and operational levels. The NIST SP800-53Ar4 is more practical in implementing controls for identifying, protecting, detecting, responding, and recovering at the operational level. The ISF Standard of Good Practice is more process- and business-oriented for managing cybersecurity with more business-understandable language, to identify gaps, and to set goals and maturity levels within organizations' strategic and tactical levels.

These best practice frameworks support the implementation of cybersecurity governance within different types of organizations and at organizational levels. The problem of the timely implementation of countermeasures, is more a project implementation process issue and is not governed within these frameworks. Governing timely implementation of countermeasure projects will be a requirement for the development of the decision support framework.

4.2 IoT best practices and principles

The generic best practices discussed above are not usable for IoT-specific adoption; however, IoT will be a part of these governance best practices. IoT adoption itself has several practical principles and frameworks to safeguard IoT implementation. Three IoT best practices can be used to complement the generic best practices are elaborated within this section.

Within IoT cybersecurity, there are upcoming cybersecurity frameworks specific to different sectors. All three frameworks are built to secure IoT devices and the infrastructure environment, next to the

existing generic cybersecurity governance frameworks that were discussed in the previous section. Three IoT best practices are the following:

Strategic principles for cybersecurity of the Internet of Things (Homeland Security, 2016). This is a set of principles for identifying organizational risk using IoT. It suggests best practices to bring this risk to an acceptable level, including cybersecurity for the IoT device, system business design, manufacture, and to maintain up-to-date systems when implemented. The following principles offer stakeholders a way to organize IoT cybersecurity challenges:

- Incorporate cybersecurity in the design phase
- Advance cybersecurity updates and vulnerability management
- Build on proven (cyber) security practices
- Prioritize (cyber) security measures according to potential impact
- Promote transparency across IoT
- Connect carefully and deliberately

These principles are usable for the following stakeholders: developers, manufacturers, service providers, and industrial and business-level consumers, including the federal government and critical infrastructure owners and operators.

Industrial Internet of Things Security Framework (Industrial Internet Consortium, 2016). The Industrial Internet consortium developed a common cybersecurity framework and an approach to assess cybersecurity in IIoT systems. This is a framework to identify, explain, and position cybersecurity-related architectures, designs, and technologies, as well as identify procedures relevant to IIoT. It describes their cybersecurity characteristics, technologies, and techniques that should be applied, methods for addressing cybersecurity, and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations.

These principles are usable for the stakeholders' IoT owners, operators, system integrators, business decision-makers, and architects. The IoT cybersecurity framework is a comprehensive, detailed guide for IoT requirements, and the framework refers to multiple standards from the ISO and NIST.

IoT Trust Framework (OnlineTrustAlliance, 2016). This is a framework from the Online Trust Alliance. The framework includes strategic principles to help secure IoT systems and data throughout the life-cycle. This framework is more for consumer-used products. The principles include cybersecurity device measures, user access, information/data protection, and cybersecurity notifications. The last principles are special options relative to the other frameworks.

These IoT best practices support different stakeholders within organizations to secure IoT systems and the surrounding ICT landscape. The adoption of this new innovative technology needs a different approach that reaches farther than traditional generic cybersecurity frameworks because there are different cybersecurity specific aspects such as security by design. Above best practices are requirements for the framework design, based on the threat profile analysis best practices frameworks and countermeasures that need to be implemented to safeguard the organization. The requirements are all IoT- and risk-specific, but these best practices do not manage the timely implementation of these requirements.

4.3 Summary

In summary, this chapter describes what is needed to govern and secure an organization from cybersecurity and IoT risk at strategic, tactical, and operational levels. Depending on the organization type, industry sector, and business, one or more best practice frameworks can be applied. For IoT, another approach is needed than a generic cybersecurity framework to safeguard against organizational risk. To this end, IoT implementation-specific best practices and principles need to be implemented. These best practices are requirements for the risk analysis part of the framework. The next chapters describe further requirements for the framework design.

All in all, the frameworks discussed above govern the cybersecurity risk, policy, activities, and processes, but do not control the timely implementation of these activities. This is a requirement for the new decision support framework.

5 Exploring the competing priorities issues for IoT cybersecurity

This chapter will elaborate on the requirements of the competing priorities problem discussed in chapter three, and on the requirement of the development of a decision support framework. The previous chapters discussed the problem of keeping organizations secure against cyber threats, and explained the struggle that organizations face in implementing cybersecurity measures in a timely manner. This thesis highlights the problem that cybersecurity projects are not well managed, and that the governance of cybersecurity projects is mostly not handled as a strategic subject. The best practices section quickly looked at the top-level cybersecurity frameworks and how they govern and control cybersecurity projects. The cybersecurity governance frameworks do not deal with managing cybersecurity projects either. This chapter focuses on how to deal with competing priorities, and the governance aspects concerning project Key Performance Indicators (KPI) within the organization.

5.1 Results of brainstorm sessions for (IoT) decision support framework

The following outlines the outputs of the brainstorming sessions as described in the methodology chapter (Chapter 2). These brainstorm sessions results were analyzed, and used for the creation of interview questions, and as requirements for developing the decision support framework. Requirements for three main categories of the framework will be described in this section, and also the following result of the brainstorm sessions as principles and requirements:

1 Cybersecurity is an organizational strategic topic. The key cybersecurity projects for protecting the organization against threats should be followed at the executive level (board level). The ICT department itself cannot make the decision itself because it has different competing objectives and cybersecurity risks are strategic issues, which need to be managed at the board level.
2 There should be a separate steering committee for key cybersecurity projects, which is *"an advisory committee usually made up of high level stakeholders and/or experts who provide guidance on key issues such as organization policy and objectives, budgetary control, marketing strategy, resource allocation, and decisions involving large expenditures."* (businessdictionary.com, 2016) This committee should be involved in business to prioritize and control cybersecurity projects, obtain commitment, and govern cybersecurity priorities within the organization.
3 The cybersecurity projects must be translated into understandable language as KPIs (risk, impact, business impact analysis (BIA), important assets) for the steering committee. The need and value to the organization must be clear.
4 Cybersecurity projects must be predictable for implementation and delays. The steering committee must have predefined project tolerances and possible risk actions to make the right decisions.
5 The cybersecurity projects have different category objectives. Not every cybersecurity project does have the same risk mitigation. For example, an awareness campaign does not protect against technical threats. Projects need to be categorized as business projects, up-keep, and resilience (this will be elaborated within the framework). There may be other categories, but these are the basics for the steering committee to understand the benefits, and also how parallel implementations can be done. For example, a business project does not have to wait until several important up-keep projects are implemented. The business must "go on" and the current environment (up-keep) cannot wait, as it is vulnerable to current threats.

Exploring the need for the new framework, the categories shown in figure 3 are defined in accordance with the results of the brainstorming sessions. Each category is the result of brainstorm session requirements. These categories will be the main framework pillars for dealing with competing cybersecurity projects:

- **Governance.** To turn cybersecurity projects into strategic ones in the entire organization (brainstorming result 1 and 2).
- **Value.** To analyze the importance of projects and project value for the organization and the order in which they should be implemented (brainstorming result 3 and 5).
- **Control**. For controlling projects, if the project threatens to exceed tolerances, then measures should be taken and the impact and risk action should be clear in advance (brainstorming result 3 and 4).

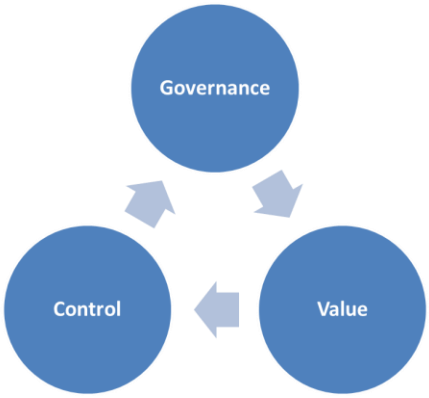

Figure 3. Three pillars

Figure 3, combined with the explored standards and best practices from the literature review regarding the research problem (Chapter three), the results of interviews with field experts and the brainstorm sessions will be used to define requirements for the solution framework.

5.2 Governance of IoT cybersecurity projects

This section outlines the results of the literature review by analyzing relevant scientific research and publications, interviews expressed as possible success factors, such as best practices in governance, which will be used for the creation of the decision support framework. It turns out that in the governance section, the cybersecurity governance for different stakeholders is very important. Outside of the cybersecurity expert field, stakeholders often lack the knowledge or have other activities to take care of besides cybersecurity. It is important that everyone works in the same direction, and with the same goal as an organizational objective.

Cybersecurity project handling

Based on the literature review, brainstorming, interviews, and review of articles, blogs, and field experience, this section will amplify project handling. Project handling means the process of the (start) realization of a project until the finished implementation (closure) of a project. To effectively protect the organization against cybersecurity threats, including those related to IoT, physical, organizational, and technical measures such as the NIST mentioned in the best practices chapter (Chapter four) are one of the key pillars. In most cases, technical measures can be implemented within interfaces in the ICT organization.

Cybersecurity is often overlooked, underestimated, or delayed. How cybersecurity is dealt with mostly depends on the maturity of the organization, the corporate culture, and the services or products that the organization provides. The research and interviews (Appendix C) show that for urgent cybersecurity matters as e.g. critical vulnerabilities, priority will be clear for carrying out cybersecurity activities to mitigate the risk of the vulnerability; this is not a problem. For urgent matters, cybersecurity awareness throughout the organization is not an issue. For the other cybersecurity projects/activities amongst the full set of competing ICT departmental projects, however, the start or timely deployment

of key cybersecurity projects to protect the organization often shifts over the years from the yearly plan cycle or cybersecurity roadmap.

According to the Security of Things World USA survey, cybersecurity budgets are too low to fill the gaps and to resolve the problem caused by the use of the same resources such as ICT and by delay of other ICT projects. The shortage of cybersecurity budget can be demonstrated by the yearly budget (SANS, 2016b), and by the survey of IoT USA (Security of Things World USA, 2016).

According to Prince-2 (Fallis, 2013), projects have a beginning and an end date. From field experience in cybersecurity projects, decisions have to be made regarding when a project should be implemented, and when it should be finished (due date). The cybersecurity project due date is defined by a cybersecurity risk analysis, compliance, or business needs. It is known that the cybersecurity project is at the expense of other ICT or business projects because not every project can run at the same time with shared resources. The correct control and sequence of cybersecurity and ICT or business projects is important. In chapter 7, this thesis offers practical guidance on how to deal with the implementation of cybersecurity projects with the aim to mitigate risk in a timely manner by implementing effective (IoT) cybersecurity counter measures.

Governance

This section is the result of literature research that is needed for developing and implementing the framework within the organization and the needs for safeguarding IoT (Chapter 3).

- ***Organization***

  Cyber cybersecurity is general known as concept, and as global risk within organizations, but there is often a lack of understanding regarding how their own organization resilience and cybersecurity affect the organization, and how this should be managed (PwC Nederland, 2014). It is often believed that this is an ICT matter, however this is no longer the case because of the strategic risk and impact. The organization must therefore be able to adapt cybersecurity. The board of directors must take control of cybersecurity strategic and operational defenses (Gregg, 2010).

  The organization must therefore be able to make changes in its strategic processes and practices. The better an organizational structure and culture can adjust its processes, the more successfully cybersecurity changes can be made to the existing practices with a risk-controlled organization as result. Cybersecurity needs specific human competences for the right decision-making and prioritization of cybersecurity projects. Most decision making stakeholders never had cybersecurity training. To support stakeholders to understand the importance of cybersecurity projects and cybersecurity is often complex in nature (PwC Nederland, 2014, p. 7). If stakeholders are not able to understand the importance of cybersecurity, this can be an organizational risk and cybersecurity projects are not implemented on time. Cybersecurity countermeasure projects are part of more protection layers e.g. a firewall and user access with a password to a system. If these cybersecurity projects are viewed individually, the larger picture is not seen with the associated risk for the organization. Involvement, understanding cybersecurity project importance and support of line and business management is therefore essential.

- ***Board-level attention***

  The traditional approach to thinking about cybersecurity in terms of building bigger walls (firewalls and antivirus software), while still necessary, is no longer sufficient. A holistic approach to cybersecurity risk management is required across the organization, its network, its supply chain, and the larger ecosystem.

Cybersecurity activities have become critical for the entire organization, as mentioned in Chapter three. The cybersecurity projects used to reduce risk must be monitored for timely implementation, and there should be cybersecurity governance to control these projects. The cybersecurity projects can no longer only be an ICT issue. Cybersecurity is a strategic risk, and the steering of this risk must be done at the board level. The right stakeholders should be aware of the risk or opportunities of cybersecurity. Therefore, the board must control the urgency and value of all cybersecurity projects. Risk decisions must be controlled at the right decision-making levels: the bottom-up approach to inform upper management about risk decisions, and the top-down approach for the right urgency and control of timely implementation.

- ***Maturity model***

  The maturity model for Cybersecurity allows to enhance organizational cybersecurity capabilities. One of the most famous maturity models is the Nolan's model of the software capability maturity model, or CMM (April, Hayes, Abran, & Dumke, 2005). The CMM is applied as a standard in many maturity models. Within ICT, this model is especially known thanks to its integration with process maturity (April et al., 2005). The maturity model is used within cybersecurity to determine the maturity level of cybersecurity processes along the metrics provided by cybersecurity standards, such as ISO/IEC 27002. The ISF Standard of Good Practice also uses maturity levels to focus on key cybersecurity attention areas within the organization (ISF, 2014). Another good practice is the Cyber Capability Maturity Model (C2M2) (Jason D. Christopher, 2014) which focuses on the implementation and management of cybersecurity practices.

  If the organization has a low maturity level, also called initial level in CMM terms, then the organization or process is often managed ad-hoc or chaotically. The higher the maturity level, the better the organization can realize a repeatable success. The lower the maturity level within an organization, the more effort should be put into the (cyber)security department processes to safeguard cybersecurity priorities and involving the cybersecurity within department processes. The higher the maturity, the better (cyber)security will be able to integrate into the existing processes. Initially, the existing processes must be prepared for adaption.

- ***Culture***

  Organizations that want to change will sooner or later be confronted with the existing organizational culture, and should adjust in the context of change processes. Organizational culture refers to how people interact with each other within the organization, the way in which decisions are implemented, and the attitude of employees towards their work, customers, suppliers, clients and colleagues. Culture is ultimately based on the standards and values of people in the organization. This will not change, but does affect changes into existing culture as implementing the decision support framework. To influence the organizational culture, leadership is needed in the form of a clear, consistent policy, ambassadors of that policy, and a stimulating personnel policy (ICTSMF, 2004, p. 180).

  The organizational culture can have a big influence on (cyber)security services. Organizations, for example, differ in the degree to which renewals are appreciated. In a stable organization, where the culture has little appreciation for innovation, it will be hard to adjust to ICT services for cybersecurity changes within the organization. If the ICT organization is unstable or immature, then can a change-minded culture seriously threaten the quality of the provided

services? An “anything goes and anything can happen” situation then arises, in which many uncontrolled changes or project portfolio objectives are not met, which can lead to a large number of malfunctions of services or cybersecurity risks (ICTSMF, 2004, p. 180).

Cybersecurity activities can be managed from (1) a process perspective, (2) from an organizational hierarchy perspective (line management), (3) from a project perspective, or (4) from a combination of these three. Organizations that often use one of the first three management systems often lack the benefits of the other. The practical choice often depends on history, culture, available skills and competencies, and personal preferences. The optimal choice can be a whole different one, but the requirements to achieve optimal choice may be very difficult to implement at the time (ICTSMF, 2004, p. 180).

The maturity levels and culture of an organization are important for change and process adjustments for cybersecurity. People are often still the weakest link within organizations; for example, people click on phishing emails or plug in unknown USB media into their systems. There is often a lack of understanding regarding cybersecurity. Influencing and connecting to existing processes and culture is therefore critical for integrating new cybersecurity processes. Even though cybersecurity is already an existing component, several steps remain important to change the cybersecurity culture and to integrate within processes. The cybersecurity team should also be prepared for organizational changes such as culture, staff turnover, and process changes. Cybersecurity must therefore remain up-to-date within the organization governance. Chapter 7.3 and 7.4 provides guidelines to this end.

5.3 Summary

The focus of this chapter was on exploring competing priorities with the use of scientific research into litrature, and brainstorm sessions. The literature study and brainstorm sessions resulted in requirements for the decision support framework. Regarding the key for success to control the timely delivery of important cybersecurity projects, the most four important categories are: (1) Cybersecurity governance within organizations to get (2) board level attention for cybersecurity projects and to (3) setup steering committees at different organizational levels to control cybersecurity projects, and (4) influence organizational culture to improve cybersecurity. These four categories will be used as requirement for the new decision support framework.

6 Interview results

Given the problem presented in Chapter three, the interviews focused on cybersecurity project priorities and timely implementation.

The interviewed organizations vary from 200-600 and from 2,000-65,000 employees. The organizations operate within different sectors in the Netherlands and abroad, with a turnover ranging from €20 million to €13 billion.

The expert interviews were based on open questions, and the interviewees could elaborate on the subject. In advance, the purpose of the Thesis was briefly explained, as was the context around the importance of cybersecurity for IoT that could impact the organization. The structure of the interviews went from a more general understanding to the specific handling of prioritizations. The interviews were therefore divided into three categories: governance, value for risk impact, and control for prioritized objectives. Each category included sub-questions to answer the research sub-questions of chapter 1.3, and to improve the results concerning the requirements for the development of the decision support framework.

	Interview 1	Interview 2	Interview 3	Interview 4	Interview 5	Interview 6	striking features
Security Governance							
IoT future adoption or demand	++	+	++	+	++	+	- as a product for critical services
Security budget benchmark	?	?	+/-	?	++	?	
Board involvement	+	+/-	++	+	++	+/-	Board level is mostly exceptional not on regular basis. More cybersecurity mature companies do have more regular board level attention
Security Mandate	+	+	+	+	+	+	Mandate is no problem for high risks. Best practice is to use mandate for special occasions only
Steering committee	-	+/-	++	+/-	++	+	Mostly common cases, mostly not a interactive process as strategic issue
Security awareness management	++	+	++	+	+	+	It varies with the individuals, most of the decision-makers are aware of the cybersecurity importance in common
Value: Security risk and impact							
Risk/threat awareness	+	+	++	+	++	++	External threat feeds
Compliance in practice	-	-	?	-/+	++	++	Security implementation for new functionalities is less difficult then for old environments. New projects mostly business added value. Mature companies will be compliant based on risk assessment of the need for best practices. They don't apply all best practices if not necessary.
Clear view on impact	-	?	++	+	++	+/-	No clear answers
View on important activities	+	++	++	-/+	++	++	Highlighted mostly cybersecurity awareness and patchmagement as key attention area's. High cybersecurity mature organizations will align protection to the risks they facing
New significant risks	++	?	++	++	++	?	New cybersecurity risk will be handled according to its impact and risk level
Control: Security priorities in practice							
Security roadmap and priority	++	+/-	++	+/-	++	+	Mostly not clear cybersecurity strategy for long term plans. Only for mature organizations. Priority based on risk reduction and available resources
Priority definition	+	+	+	+/-	++	+	Based on impact and benefit. No formal risk assessment based on CISO profession.
Project steering committee	-	+	++	-	++	+	If company cybersecurity awareness is high cybersecurity projects are not discussed on competition. Cybersecurity steering is mostly within ICT department and escalation to strategic level. Few alignments with business steering committee. External control/oversight outside ICT is important for protection of cybersecurity between competing priorities
Prevail security activities	++	++	++	++	++	++	Focus is on importance of patching systems, this is well governed as priority within organizations
Security activities delay's	?	?	?	+/-	?	+	No clear answers
Competing priorities	-/+	-/+	++	-/+	++	+	For business cybersecurity mostly not an issue for other activities this can be a problem and business case is important. Bottleneck is cybersecurity knowledge and resources External ICT resources can be a problem, because their lag of internal organization knowledge and new functionality must be adopted by internal resource team if not engaged. Cybersecurity mature organizations involve alignment with business. Security teams are sized to handle cybersecurity needs, dedicated cybersecurity teams.
Increased risk by delay	?	?	++	+	?	++	No issue, or no comment
Steering project risks	+	+	++	+	++	++	Escalation procedure, no clear process for cybersecurity projects escalation. Cybersecurity mature organizations do have processes in place to escalate problems. Question is if this will be used.

Figure 4. Table of summarizing the interview results

Figure 4 summarizes the interview results and striking features. The "– or ?" sign indicates an attention area of the given topic. The "+" sign indicates a good practice.

From a cybersecurity point of view, often No answers were given to the questions that revealed vulnerabilities or organizational risk. The detailed outcomes of the three topics and sub-questions are presented in Annex F.

6.1 Summary of the interview results

This topic is a summary of the interview results of Appendix C. Enterprise organizations are more cybersecurity-mature than med-sized organizations. They have better governance of the cybersecurity aspect within the organizations. The medium-sized organizations seem to be more pragmatic about implementing projects. For high-priority cybersecurity projects or activities with a direct organizational threat, priority is not an issue. Concerning the cybersecurity maturity level of the medium-sized organizations, the question is whether they have the full knowledge of cybersecurity best practices to protect their important assets. This is because not every interviewee was familiar with question nine SANS.ORG (SANS, 2016a) critical controls best practice. SANS.ORG is one of the most general known best practices for cybersecurity.

Most interviewees stated that their organization did not have problems with timely delivery of cybersecurity projects, or they did not want to answer this question. Not answering some questions meant generally that the specific question wasn't applicable or the information was confidential. Companies that do not have problems have dedicated cybersecurity teams or use ICT services managed by external contractors. However, almost every interviewee indicated that his or her organization struggled with competitive project priorities. The cause was mostly budget-related or the overruling of priorities by ICT stakeholders. Interviewees mentioned the best practice of using special cybersecurity steering groups and board-level attention.

This question *"What is the business impact and/or societal impact if IoT cybersecurity is not handled and prioritized as needed within organizations?"* is hard to answer in detail. Most interviewees answered that it does impact the organization, but they did not know the figures. How bigger the organizations cybersecurity maturity level, the more the organization has also categorized the business impact into different categorized subjects such as local damage, site damage, country level damage etc. Overall, cybersecurity does have attention and the running of projects depends on the capabilities and cybersecurity risk knowledge of important stakeholders and individuals within the ICT department. The individual knowledge level is important because there are not many organizations that manage key cybersecurity projects at the board level as a strategic topic. This means that cybersecurity project steering and decision-making are often done at the ICT department level.

The detailed interview research results and the resulting decisions support framework requirements are described in Appendix C. The extracted requirements for the development of the decision support framework can be found in Appendix B.

7 Designing a management decision support framework

The research sub-question "Given the answers to the previous questions, how would a generic cybersecurity management decision support framework look like that also covers IoT for organizations?" will be discussed in this chapter. The outcomes of the sub-questions are translated into requirements. The requirements are used to develop a generic cybersecurity management decision support framework.

What is a management decision support framework ?

- The definition of management: The process of dealing with or controlling things or people (en.oxforddictionaries.com, 2016).
- The definition of decision: A style of behavior that is appropriate to the achievement of given goals, within the limits imposed by given conditions and constraints (Hyde, 1999).
- The definition of support: Give assistance to (en.oxforddictionaries.com, 2016d).
- The definition of framework: A basic structure underlying a system, concept, or text (en.oxforddictionaries.com, 2016b).

In summary, the decision support framework is a structured concept that gives assistance to management to deal with or control achievements regarding given goals with the limits of given conditions and constraints.

The framework consists of three pillars shown in figure 6, that are crucial for effective management of key cybersecurity activities or projects. The framework is built for CISO as guidance to govern cybersecurity activities through the whole organization and to monitor and control at the strategic board level.

Board/steering committee: With this framework, board members have the benefit of a simple and effective dashboard for managing strategic cybersecurity risk. Technical cybersecurity risk is translated into understandable organizational risk and predefined corrective actions when decisions need to be made if performance indicators are not in line with the objective.

CISO. With this framework, the CISO has practical guidelines to roll out the framework within the organization and to initiate cybersecurity projects translated to strategic topics of the organization.

The framework should provide a solution to the research goal: *"To develop an (IoT) management decision support framework to safeguard businesses in a timely manner before possibly high-impact cybersecurity incidents become a reality."* The framework is suitable for IoT management as well traditional ICT cybersecurity management. The management of cybersecurity projects at the strategic level is equal to cybersecurity IoT as cybersecurity ICT, because cybersecurity project management should be based on the organizational impact. This is the same for cybersecurity ICT and IoT. Only the countermeasures are different.

This management decision support framework will operationalize and sustain the cybersecurity strategy within organizations at different management levels. The framework will be useful for stakeholder management to take well-considered cybersecurity decisions between competing business priorities. Having a framework will not solve the organizational governance of implementing the framework, however. The best-practice four-step approach presented in chapter (Chapter 7.4) will guide a successful implementation of the framework.

7.2 Requirements

Building an management decision support framework, this must be based on the right starting points for effective use. Therefore, it is important to build the framework on requirements of the research results. These requirements are the elaboration of interviews, brainstorm sessions and literature study. As shown in figure 5.

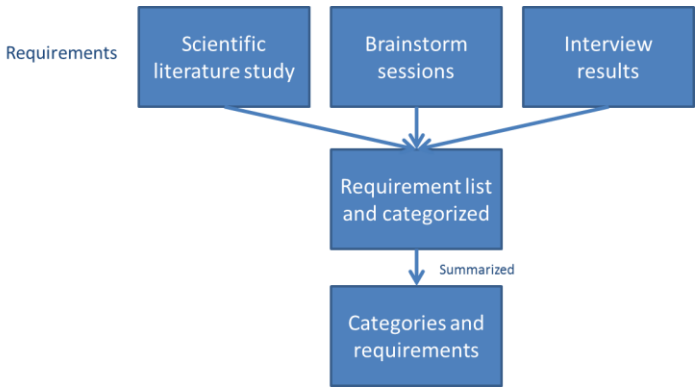

Figure 5. Framework requirements process

The outcome is a 35 item requirement list as shown in Appendix B. The 35 requirements are reviewed and summarized into category groups of the framework. The category group names are based on the main subject of the category requirements. For example Steering committee for cybersecurity requirement is named as category "steering committee". The following requirements and category groups are defined:

Governance

Requirements for the governance pillar figure 6 of the framework. The number defines the framework topics and the category of the key attention areas of the topic.

No.	Category	Requirement
G1	Steering committee	Steering committee for cybersecurity projects at different organizational levels (ICT, business, and board)
G2	KPI Dashboard	KPI such as strategic roadmap and control dashboard for decision-makers
G3	Stakeholder awareness	Specific stakeholder cybersecurity awareness approach
G4	Cybersecurity business risk language	Translate organization's cybersecurity risk profile and risk attitude or appetite into understandable business language

Value

Requirements for the value pillar figure 6 of the framework.

No.	Category	Requirement
V1	Risk framework	Inventory of roadmap projects in advance from compliance requirements, risk, threats, best practices, innovation, or business requirements
V2	Define KPI	Definition of risk, impact, priority, sequence, business case, project tolerance, and due dates
V3	Category	Project partitioning in different categories for business objectives, upkeep to stay secure, and resilience to continue to improve cybersecurity against changing cyber threats

Control

Requirements for the control pillar figure 6 of the framework.

No.	Category	Requirement
C1	Cybersecurity boundary	Clear expectation about the organizational cybersecurity risk tolerance and appetite, the timeframe of projects, and definition of proactive indicators of due date failures
C2	Control measures	Proactive and reactive countermeasures for project boundary and due date failures

The requirements are used to develop the management decision support framework. Development of the framework is derived from scientific research into literature, brainstorming, and interviews combined with extended experience, creativity, intuition, and problem solving capabilities of the researcher.

7.3 Management decision support framework

The management decision support framework is developed by the Thesis researcher extended experience and the use of scientific literature concerning best practices. The developed framework is further elaborated on the three strategic topics of governance, value, and control, as shown in figure 6 as a result of the brainstorm sessions mentioned in chapter 5.1. These strategic topics, also called the three pillar framework, are derived from chapter 5.1 where the key to success is defined for the monitor and control of cyber security projects.

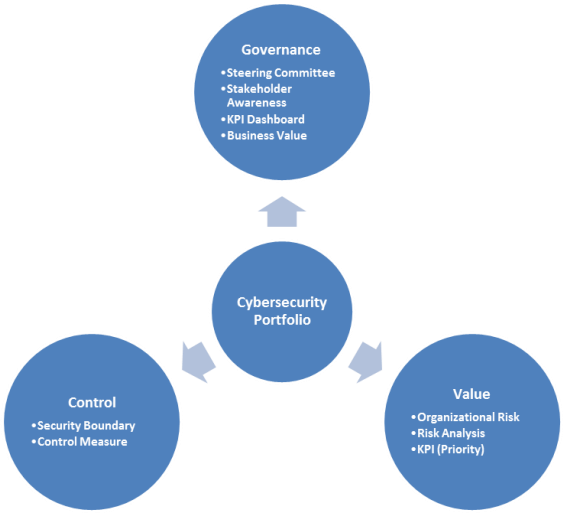

Figure 6. Three pillar framework (Governance, Value and Control)

Value supports translating cybersecurity threats into an understandable business langue to control threats such as organizational risk. Governance supports effective management of the organizational cybersecurity risk at different organizational levels: strategic, tactical, and operational. Control is needed if key cybersecurity activities or projects exceed the cybersecurity project boundaries. Figure 7 shows the overall management decision support framework and in the next sections each pillar will be elaborated.

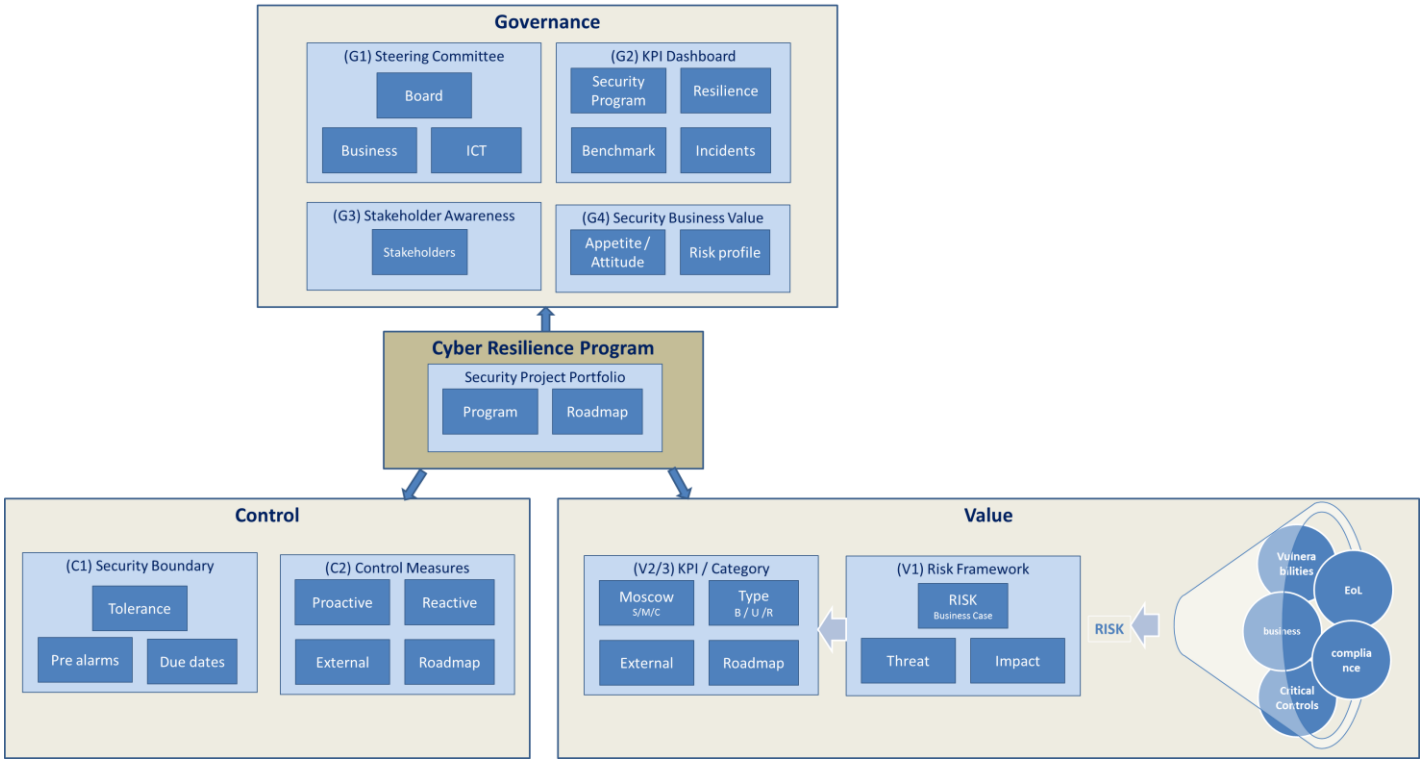

Figure 7. Management decision support framework

Governance

The governance section consists of the steering committee, the KPI dashboard, the cybersecurity business value, and stakeholder awareness. These topics are shown in Figure 8. They will be elaborated in this governance section.

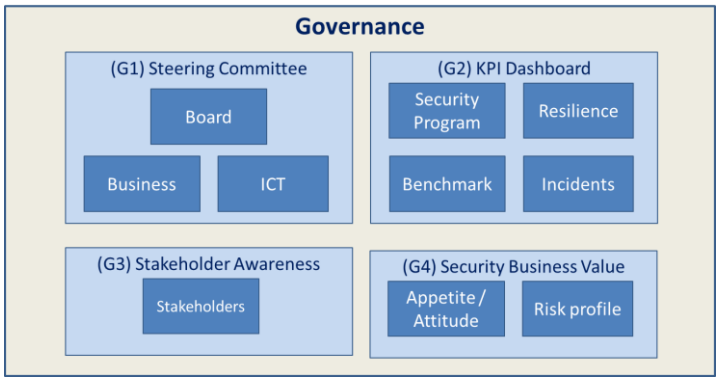

Figure 8. Governance pillar

Requirement as input for the framework:

No.	Category	Requirement
G1	Steering committee	Steering committee for cybersecurity projects at different organizational levels (ICT, business, and board)

The G1 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

Project board at different organizational levels

To successfully manage cybersecurity within the organization, there must be engagement both top-down and bottom-up. To successfully roll out the cybersecurity program, there should be a cybersecurity program at the executive/board level, a project board at the business/process level, and a

project board at the implementation/operations level, as shown in figure 9. The NIST Cyber Security Framework (NIST, 2014a) supports this approach in detail.

Figure 9. Organization levels for integration of the cybersecurity program

Board/executive level

The executive level communicates the mission priorities, available resources, and overall risk tolerance to the business/process level (NIST, 2014a, p. 12).

In today's world, it would be hard to suggest that cybersecurity should not be part of any organization's enterprise risk management function or part of any director's overseeing duties. The board or an executive member should be responsible for cybersecurity. Based on best practices proposed by Robert Gregg (Gregg, 2010) and Paul Ferillo (Ferrillo, 2014), the basic questions that directors should ask when they want to successful set up their cybersecurity steering committee and/or cybersecurity strategy are the following:

1. Set up the cyber committee. What part of the board should handle the examination of cybersecurity risk? The whole board, or should responsibility be assigned, or should the board create a "cyber committee" to exclusively deal with these issues?
2. Own the problem. Cyber risk must not be relegated to an ICT issue. Senior executives with cross-departmental authority must take strategic and operational control of the cyber risk problem. The CFO is usually the right individual to "own" and lead this effort.
3. Hold regular meetings. How often should the board (or committee) be receiving cybersecurity briefings? In this world, cybersecurity breaches are reported daily; are quarterly briefings enough? Should the board be receiving monthly briefings? Because of the unique and technical nature of the cybersecurity risk, meetings must be held regularly and ideally in person. It is often the case that such teams need to develop a common vocabulary to address issues, since often ICT cybersecurity people are used to "speaking a different language" than others.
4. Create a cyber risk team. Because of the breadth and complexity of cybersecurity issues, the responsible executive needs to form and lead a team that draws from relevant domain expertise across all functional areas of the organization. Given the sheer complexity and magnitude of many cybersecurity issues, depending on the size and risk importance the board should appoint its own "cyber advisors" internal or external, to consult on cybersecurity issues.
5. Develop a cross-functional cyber risk management plan. Senior executive management's adoption of a cyber risk plan will foster the proper level of visibility and understanding of the level of financial exposure inherent to cyber risk. In most organizations, it is the lack of risk awareness and appreciation that leads to inadequate management of the issue.
6. Create a cyber risk budget. The lack of appreciation for cyber risk by senior executives is partly because the financial exposure is often not quantified. It is recommended that the CFO

quantify the organization's cyber risk using a proposed model, and then base the budget for managing cyber risk as a percentage of the exposure. What would the worst-case cyber incident cost the organization in terms of lost business (because of downtime of systems that were attacked and need to be brought back and because of the harm to the organization's reputation because of the attack)?

7. What are the greatest threats and risk to the organization's highest-value cyber assets? Does the organization's human and financial capital line up with protecting those high-value assets?
8. What sort of "cyber due diligence" does the organization perform with respect to its third-party service providers and vendors?
9. Implement and audit performance. Cyber risk is a moving target. Once the plan is created to manage cyber risk and implementation is underway, the CFO must ensure that progress and performance are regularly assessed and periodically formally audited. In many industries – primarily financial services and health care – this audit process is consistent with and will contribute to regulatory compliance.

The following are executive cyber resilience questions to consider:

10. What is the organization's volume of cybersecurity incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? What is the time taken and cost to respond to those incidents?
11. What is the organization's specific cyber incident plan, and how will it respond to customers, clients, vendors, the media, regulators, law enforcement, and shareholders? Does the organization have a crisis management plan to inform and respond to its constituencies, as well as the media (both print and electronic/high-activity bloggers/TV)? Finally, has the cyber incident plan been tested (or "war-gamed") so that it is ready to be put into place at a moment's notice?
12. What cybersecurity training should the organization give its employees?
13. In a mergers and acquisitions context, what is the level of cyber due diligence that is done as part of the consideration of any acquisition?
14. Has the organization performed an analysis of the "cybersecurity-robustness" of its products and services to analyze potential vulnerabilities that could be exploited by hackers?
15. Finally, should the organization consider adopting, in whole or in part, the NIST cybersecurity framework or comparable framework as a way or method of showing affirmative action to protect the organization's IP assets?

There are more topics, but these will be covered within the governance KPI solution. The executive responsible should be motivated to take these actions. If not, he or she exposes his or her organization to huge risk of loss financially, as well as negative effects on the organization's reputation and brand.

Cybersecurity governance program

Given the challenges discussed in Chapter three, organizations should design a resilience program to address these vital issues. The program has to analyze the cybersecurity resilience baseline and organizational-facing threats to decide which countermeasures need to be implemented to reduce the risk. The risk should be translated into information assets and business risk. This helps senior business stakeholders understand what is at risk and why this is important. Defining business risk themes rather than technology will also improve understanding of and commitment to the change program. In addition, providing pragmatic options, with different risk and resource implications, will help senior management to understand the implicit risk appetite, and to make sure the program as a whole aligns with the risk appetite. Moreover, building modules into the project plan to engage with each individual business line on differentiated protections helps to ensure that business managers take responsibility

for making decisions on cybersecurity risk. This governance structure will take cybersecurity decisions outside of ICT because they will be owned by the business.

To launch an effective program, organizations have to understand the full scope of it. They do this by defining program goals and deciding how the cybersecurity organization should operate. Then, they adjust how to get there using a plan, considering the major risk and resource consequences, and ensuring that the roadmap is aligned with the technology needed to deliver the business imperative. Finally, the senior business stakeholders can move to execution to ensure control of the progress and have sustained engagement across cybersecurity issues, ICT, and business functions (McKinsey, 2015).

Strategic cybersecurity program or portfolio

This section elaborates on the cyber resilience program, as shown in Figure 10.

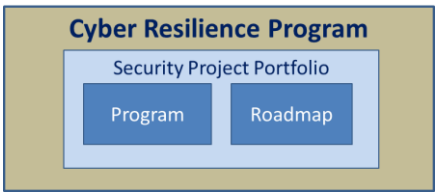

Figure 10. Cyber resilience program

This program is a collection of projects that together achieve a beneficial change for an organization (Fallis, 2013, p. 6). All the practices critical to ensuring an effective business-technology program are equally important for a cybersecurity program. An organization must appoint a single responsible program manager. It must define work packages with accountable initiatives. Each initiative must have an owner who will be accountable and be dedicated to the initiative charter that lays out expected outcomes and a project plan with milestones, dependencies, and specific resource requirements. The initiatives must be controlled in an overall road map or program that provides insight into resources across projects and dependencies between these projects.

Traditionally, cybersecurity programs are built on different types of controls and compliance requirements that need to be implemented. However, to truly integrate cybersecurity into business processes and strategies, a full digital resilience plan should include initiatives aligned by business as well as by technology controls. If the business understands the importance of information assets, business risk, and creating new technology capabilities, it will better understand the focus and will follow an effective cybersecurity change program. Setting up a successful project program was described in Chapter four as a project portfolio.

Business/process level

The business and/or process level uses risk management and business impact assessment to collaborate with the operational level. Technical countermeasures are translated into risk that helps to communicate business needs and create a risk profile. The business level management reports to the executive level to inform the organization's overall risk and business impact. At the executive level, there will be a steering committee for the strategic cybersecurity project portfolio. How to manage this portfolio will be explained in the next section (NIST, 2014a).

Steering committee / project board

A steering committee is also called a project board within the best practices of Prince-2 (Fallis, 2013). The project board is responsible to corporate or program management for the overall direction and management of the project, and has responsibility and authority for the project within the project mandate set by corporate or program management.

The project board is a decision-making body, not a discussion group. For this reason, it is not a good idea to allow the project board to grow too large. Ideally, it should not grow beyond three to six people, even for a large project. It may not always be possible to restrict it to this size, but for example, a separate user group can often be set up, which will appoint one of its members to act as Senior User on the project board.

Key questions

- If the project is part of a program, will the program management team fulfill any roles on the project board?
- Does the proposed executive have the financial and functional authority necessary to adequately support the project?
- Do the appointees have the skills and knowledge required to undertake their task?

Fundamental principles

- An essential for a well-run project is that every individual involved in the management of the project understands and agrees regarding who is accountable to whom for what, who is responsible for what, and what the reporting and communication lines are.
- There must be agreement and acceptance from everyone regarding their roles and responsibilities.
- There should be no gaps in responsibilities once the roles have been tailored; someone should be clearly responsible for each given management aspect.
- Confirm project tolerances with corporate or program management.
- Commit project resources required for the next project or stage.
- One project board responsibility that should receive careful consideration is approving and funding changes.

The project board is ultimately responsible for ensuring that the project remains on track to deliver the desired outcome of the required quality to meet the business case defined in the project initiation document (Fallis, 2013, p. 395).

Implementation/operations level (ICT)

The implementation/operations level communicates the project implementation progress to the business/process level. At this level, the technical projects will be implemented and managed between the ICT projects with the level's own ICT project program. Managing cybersecurity projects on this ICT layer, the organization is fully dependent on efforts by individuals and cybersecurity awareness of stakeholders and key cybersecurity projects not governed as strategic topics outside of ICT.

Requirement as input for the framework:

No.	Category	Requirement
G2	KPI Dashboard	Key performance indicators such as a strategic roadmap and monitor & control dashboard for decision-makers

The G2 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

A cybersecurity dashboard will help to steer the organization towards the desired cybersecurity position.

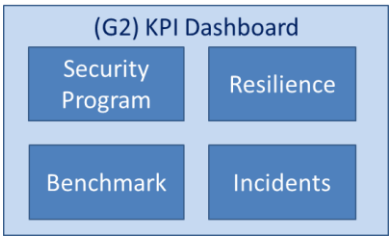

Figure 11. KPI Dashboard

Many organizations have struggled with creating an understandable cybersecurity dashboard. Often a cybersecurity dashboard is used by decision-maker with KPI to monitor and control cybersecurity projects. The complexity around cybersecurity is large and the audience often does not know what KPI indicators must be present within a dashboard for correct decision-making. The cybersecurity dashboard, shown in figure 11, must be adapted to the different target groups, as mentioned in the governance section. The above model has three target groups: the board, business, and operations.

For this decision-making model, the focus is on cybersecurity projects. However, at the board level, there are multiple cybersecurity KPI within the dashboard. Making an understandable cybersecurity dashboard is key, and it is also difficult. For the KPI dashboard in this study, best practices are used from different organizations, such as KPMG, EY, and ISACA. The different cybersecurity dashboard KPI to address are:

- Business impact of cyber risk
    - To inform executive stakeholders about the business impact and current level of cybersecurity risk to the organization and strategy.
- Cybersecurity threats
    - How well do we protect high-value information, especially given today's increasingly cyber threats? And are we in control of cybersecurity in the value chain?
    - What is the status of our cyber resilience capabilities compared to the current and expected threat level?
- Business objectives
    - Is our cybersecurity strategy aligned with our business objectives? And are we spending on the right cybersecurity areas of priorities?
    - Is our cybersecurity focused on protecting the assets that support the business objectives or processes that make money for our organization?
- Cyber resilience
    - Would we know if we were the victims of a breach?
    - How many cyber incidents do we detect in a normal week, and what types are they?
    - How comprehensive is our cyber incident process? Do we exercise the cybersecurity incident process?
    - How do we measure the effectiveness of our cybersecurity program?
- Cyber program and projects
    - How does our cybersecurity program apply industry standards and best practices? And what is our plan to address identified risk?
    - What is the threshold for notifying our executive leadership?
- Benchmark
    - Is our cybersecurity function appropriately organized, trained, equipped, staffed, and funded? And how do our measures and investments compare to the rest of our sector?

Defining the risk strategy and levels of acceptable risk together with executive engagement enables the definition of business-aligned needs and cost-effective management. Regular communication between the executive and accountable owners to manage cyber risk provides awareness of current risk and affects the organization and associated business impact positively (NCSC-NZ, 2013).

The above topics will support the board in strategically controlling cybersecurity. For more details on controlling the projects, the KPIs of value can be used within the board. These KPIs will translate the project need into understandable organizational risk.

Requirement as input for the framework:

No.	Category	Requirement
G3	Stakeholder awareness	Specific stakeholder cybersecurity awareness approach

The G3 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

Stakeholder awareness, as shown in Figure 12, is part of the framework and one of the most important topics for success. Cybersecurity within the organization is a difficult subject. Managers within organizations should adopt new business processes regularly, and other departments, such as legal, communications, and sales, need to be involved in the event of a cybersecurity incident. Convincing managers to take part in cybersecurity activities can be difficult. Managers often feel overruled by corporate initiatives; agile working, lean management, cost reduction programs, etc. To cut through this, the most senior managers, including the CEO, must be actively engaged in supporting the cybersecurity strategy.

Figure 12. Stakeholder awareness

The complexity of cybersecurity makes it hard to engage effectively with the senior executive team. Senior business executives already consider ICT managers to belong to a priesthood that uses impenetrable jargon to describe mysterious issues, and cybersecurity is even more confusing. This stakeholder awareness approach must support all different stakeholders to be aware of and well informed about the importance of cybersecurity.

Approaching stakeholders

First, the key stakeholders need to be identified. To do this, Mendelow's best practice approach is useful. This approach was described in Appendix D topic "Power vs. Interest Matrix". There are different techniques to approach different stakeholders. Weick proposes the following best practice approach, called sense making (Weick, 1995): *"The basic idea of sense making is that reality is an ongoing accomplishment that emerges from efforts to create order and make retrospective sense of what occurs."* (Weick, 1993: 635) This is suitable for approaching different stakeholders involved within the change strategy to implement and maintain this framework. Within organization studies, the concept of sense making was first used to focus attention on the largely cognitive activity of framing experienced situations as meaningful. It is a collaborative process of creating shared awareness and understanding out of different individuals' perspectives and varied interests. Weick's collaborative properties to adapt are to be found in Appendix E.

Weick and Mendelow' method will help to identify the key stakeholders and influence or feed them with information that is relevant to their objectives to create cybersecurity awareness and acceptance.

Requirement as input for the framework:

No.	Category	Requirement
G4	Cybersecurity business risk language	Translate organization's cybersecurity risk profile and risk attitude or appetite into understandable business language.

The G4 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities. To create an understandable cybersecurity risk language, one must bring together the business, strategy, risk, ICT, and cybersecurity to identify and prioritize risk using a common frame of reference. Figure 13 shows the cybersecurity business value section of the governance category. This will be described as appetite and risk profile.

Fig 13. Cybersecurity business value

Appetite/attitude

For business executives to understand cybersecurity, the value-at-risk from cyber-attacks is key, next to the high-impact cybersecurity incidents affecting key information assets within important business processes. The executives will better understand which information assets are the most important in this context and why, and that the risk of those assets being exposed should drive the level of protection. Then, the executives will better understand the need for cybersecurity investments. The CISO helps the business take complex balanced decisions, as shown within Figure 14, and has the authority to supervise the implementation of the initiatives with ICT and business and to escalate potential cybersecurity project risks, where there are roadblocks and delays. When aligning the board with cybersecurity, the CIO is comfortable justifying the cybersecurity expenditure and can defend it as part of the overall portfolio of ICT initiatives.

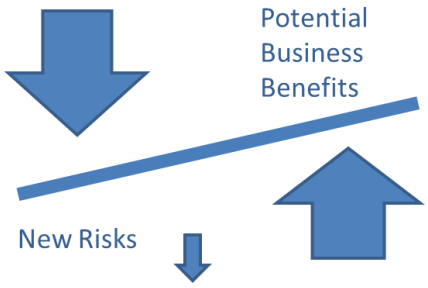

Fig 14. Balances organizational risk and benefits (Ernst & Young, 2014)

A cybersecurity roadmap starts by assessing the state of things and, from there, developing a perspective on information assets and business risk. This helps senior business leaders understand what is at risk and why this is important. Creating widespread support around business themes rather than technology will also improve the understanding of and commitment to the required change. Providing pragmatic options, with different risk and resource implications, will draw out senior management's implicit risk appetite and ensure that the program as a whole is aligned with it.

To make sure that cybersecurity is understandable within the business, CISO must build their prioritization efforts around business concepts rather than technology.

Business language (risk profile)

Talking about cybersecurity risk with business leaders is tough when one talks about vulnerabilities, pour patching, flat network, etc. A better way to talk about business risk is to ask questions such as the following: How would customers react if an organization allowed attackers to steal their personal or critical data? And how much does the competitor benefit from gaining access to our organization's intellectual property secrets?

Then business leaders will understand cybersecurity if one talks about valuable information assets, attackers, and business impact when prioritizing an activity. Another approach is to use the organizational value chain and risk classification. A business value chain identifies each process step that constitutes the core business and creates the primary value stream. The value stream in banks, for example, taking orders from customers, and opening an account in a bank. For each step, a classification of business risk reveals important questions to ask:

- Within this step, is there digital information that would cause reputational damage if publicly exposed?
- Could sensitive business information be disclosed about this step?
- Are there opportunities for cyber-fraud?
- Is there potential for business disruption or data corruption?
- Does this step use intellectual property that might be valuable to competitors?
- Could regulatory actions occur?

These guidelines support the cybersecurity team or CISO in developing a first view of the organizational risk appetite with the use of information assets and the risk profile of the cybersecurity program. These guidelines help business leaders to comprehend the business risk with an understandable language (McKinsey, 2015).

Cybersecurity balance

Balancing cost, risk, and value enables a balance between cost and value, as seen in figure 14. EY's cyber program management enables organizations to perform the balancing act of reducing costs while identifying gaps in existing cybersecurity capabilities. This is a good best practice to use to achieve the right balance. The balance findings can help to make strategic prioritized investments to address business needs, increase the organization value, and keep the organization secure. Balancing cost, risk, and value concerns the following questions:

Cost. Are our cybersecurity capabilities efficient and effective? Do we have the right resources, right initiatives, processes, and technologies? And do we have the right investments?

Risk. Does our cybersecurity program currently manage enterprise cybersecurity risk? Adequately protect us from new emerging threats? Identify gaps and remediate root cause cybersecurity issues? And proactively respond to changes in the business and regulatory environments?

Value. Will our cybersecurity program keep us competitive, and protect brand image and value? Protect the assets of the most importance to the organization? Support strategic objectives and enable new business initiatives?

A best practice for cybersecurity balance is to use EY's Cyber Program Management framework, titled "Identify ways to get ahead of cybercrime." (Ernst & Young, 2014)

Important value assets

The value chain of the framework identifies the important value assets, the risk, the organizational impact, and the KPI for managing the cybersecurity program. Figure 15 shows the different value subjects to manage the framework.

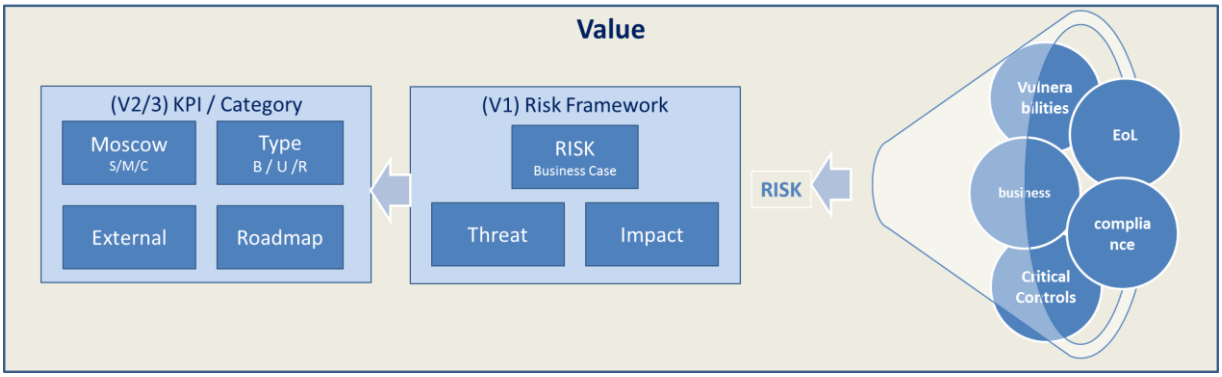

Figure 15. Value pillar of the framework

As input for the board or cybersecurity program level, the most important ICT service assets, the ICT components that are critical in the organizational value chain, should be identified. This can be done with e.g. a Business Impact Analysis (BIA). The BIA determines how key disruption risk could affect an organization's operations, and identifies and quantifies the capabilities that would be needed to manage it. The BIA risk assessment technique is described in ISO/IEC 31010:2009 (ISO/IEC, 2009, p. 42). Otherwise, if the BIA already done within current Information Technology Infrastructure Library (ITIL) processes, this is a best practice method often used within ICT service departments. This can be used in combination with the cybersecurity risk assessment.

Requirement as input for the framework:

No.	Category	Requirement
V1	Risk framework	Inventory of roadmap projects in advance to compliance, risk, threats, best practices, innovation, or business requirements

The V1 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

To launch an effective program, organizations first have to set the agenda, which means understanding the full scope of the program, defining their goals, and deciding how the cybersecurity function should operate. This is done at the governance layer. Then they need to set out the plan for how to get there, considering the major risk/resource trade-offs and ensuring that the road map is aligned with both business imperatives and the technology needed to deliver. Organizations cannot start an effective program if they do not know where to start. A gap analysis must always be done first based on organizationally suitable frameworks, best practices, vulnerabilities, and risk assessment regarding the threat and impact. Figure 16 represents the gap analysis input for the risk framework.

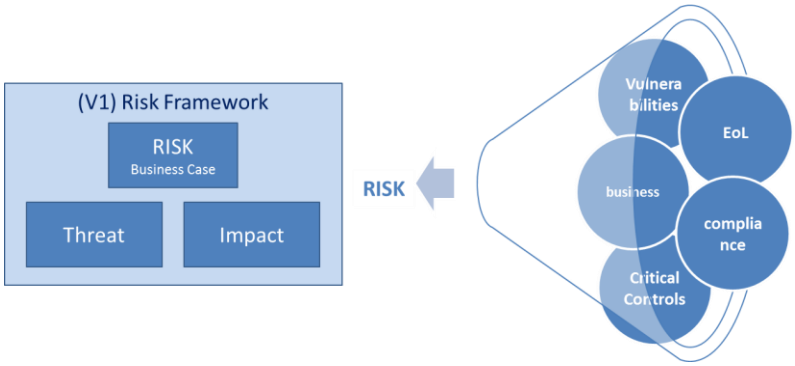

Figure 16. Risk framework and gap analysis

Off-the-shelf frameworks, best practice measurements and guidance, such as ISO/IEC 27001:2015(ISO/IEC, 2013b) and the US National Institute of Science and Technology (NIST)(NIST, 2016a), which were mentioned in the best practices chapter, can be valuable in elaborating how organizations act with cybersecurity activities, but even they have their scope limitations. For example, organizations underestimate the attention that is required for product cybersecurity and many types of third-party risk. Almost all such frameworks focus on technology risk. Other frameworks, such as the ISF Standard of Good Practice(ISF, 2013), integrate critical business processes and maturity levels. It is important not only to select one, but also to select organization-specific suitable frameworks. This can be more than one to cover the organizational risk profile. The suitable framework(s) must support the overall cybersecurity strategy with its supporting business objectives. Traditional cybersecurity is based on implementing countermeasures or upgrades. To successfully integrate cybersecurity into business processes and strategies, a digital resilience plan should include initiatives aligned with countermeasures and business as well.

The risk framework will be fed with the best suitable framework, best practices, vulnerability assessments, etc. This will be suitable to identify the cybersecurity needs of the organization. This will be further described in the next section.

Requirement as input for the framework:

No.	Category	Requirement
V2	Defining KPI	Definition of risk, impact, priority, sequence, business case, project tolerance, and due dates.

The V2 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

Defining KPI creates the preconditions for effective decision management and success in the implementation of key cybersecurity projects or activities. Figure 17 shows the main KPI and category topics.

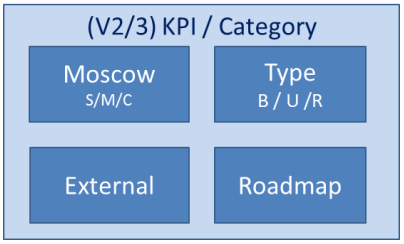

Figure 17. KPI/Category

The business value defined into KPI help to identify risk using best practices and different risk methods. The actions needed to mitigate the risk will be translated and prioritized into business-understandable language. The business, ICT, executive, and CISO all need a common language and set of mechanisms to assess risk, evaluate potential protection, and support KPI to make trade-offs. From identifying the needed cybersecurity project or activity to putting it on the strategic roadmap, the following six steps, shown in figure 18, concern effective cybersecurity strategy and decision-making controls in the cybersecurity program.

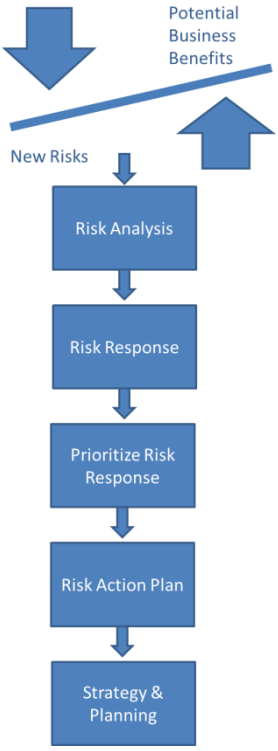

Figure 18. Risk balance and process of planning

Six steps for the defining the cybersecurity KPIs as input for steering committees

1 *Organization risk balance.* To understand one's organization's risk attitude or appetite as defined within the governance requirement G4 Security Business Risk Language.

2 *Risk analysis.* Understanding one's organization's risk exposure, critical information assets, assessing the maturity of current cybersecurity, and identifying areas for improvement. Best practices that are aligned with one's organization can be used, as mentioned within the value requirement V1 Risk Framework. Risk analysis is not done with only one framework. Instead, it consists of multiple analyses of different frameworks and best practices to analyze threats, vulnerabilities, attack tree(Ten, Liu, & Govindarasu, 2007), and process maturity levels. Different frameworks support risk assessments:

- See different frameworks V1 "Risk Frameworks"
- Vulnerability Assessment of Cybersecurity using fault-tree and attack tree analysis, for in-depth defense or multiple controls analysis (Ten et al., 2007). Fault-tree/attack tree analysis it to define the steps that are needed to compromise the important asset, to identify the level of protection.
- One best practice is the Information Security Risk Assessment Process for Internal Affairs from the New Zealand Government . This risk assessment process is a combination of the ISO/IEC27005:2013, OCTAVE and SABSA risk assessment methodologies. (Internal affairs New Zealand, 2014)

3 *Risk Response.* Once the risk analysis is complete, the residual risk can be evaluated against the risk tolerance levels. The identification of the risk response will be done by the project board or business owner. The risk response can be avoid, treat, transfer, or accept (Internal affairs New Zealand, 2014). Often there will be several controls that can be implemented as deterrent, preventive, detective, and corrective controls. These can be implemented either individually or in combination with each other, as done within (2) analysis with attack tree, to reduce the likelihood and/or impact of an attack.
    - Risk response balance is done at the directive board and project board levels.
    - Risk response advice and decisions done or delegated by the directive board level.
4 *Prioritize risk response*. The risk assessment (2) should clearly identify the priority and risk response (3) and the actions needed to implement the proposed controls. With a risk analysis in combination with e.g. attack tree analysis of the important assets, the priority can be defined. Traditional risk assessments can be used, such as ISO 27005(ISO/IEC, 2011). This is great for the cybersecurity expert, but for board members this is not always understandable. It is better to translate the cybersecurity priority into understandable language, such as the MoSCoW principles, in combination with categorization and added value to lower the business risk.
    - The MoSCoW is a kind of numerical assignment method and a generally known prioritization technique used e.g. in management, project management, and software development. MoSCoW contains the highest degree of confidence and is easy to use. The idea of MoScoW is that it groups all requirements into four priority groups: "MUST have", "SHOULD have", "COULD have", and "WON'T have." (Agilebusiness, 2008 DSDM Atern Handbook)
    - The external KPI is the influence of external regulation compliance that can also be part of project category V3 and priority groups of MoSCoW.
5 *Risk action plan.* Project action plans are the risk tolerance parameters for the project board when it must control the project in case of project or program risk. The project risk response process should involve identifying and evaluating a range of options for treating project implementation-related risk. When preparing acceptable project risk tolerances, which is another name for risk appetite (Fallis, 2013, p. 252), the project board should determine the acceptable amount of risk that it is prepared to tolerate, for example regarding budget, effect on other parts of projects, or political embarrassment. The risk action plan will define the tolerance parameters versus organizational risk. Risk tolerance parameters include time to completion (due date), countermeasures for e.g. resource availability or other organizational cybersecurity risk reduction methods, and timescale and/or cost balance to achieve product quality.
6 *Strategy and planning.* The strategy and planning are the input for the overall project program or project board. Based on the project priority risk response (point 4), the MoSCoW principles, and combination of the project categorization; category business objective: is the project supporting the business objectives, category upkeep: to stay secure or category resilience: tracking innovations against threats. Both the priority and category will be the input for the project program or portfolio to define the right order or sequence to implement the projects. All three categories have to be parallel topics on the overall project program. The overall program is where all organizational ICT projects come together. They are parallel because one cannot forget or postpone "Must" upkeep projects versus new "Must" business objective cybersecurity projects. Because the risk exposure of a vulnerable system in the upkeep cybersecurity projects is an organizational risk that can't be postponed because the threat won't wait until the project is implemented, and the business project has to go live, but can't go live without proper cybersecurity protection. However, if a business project replaces or supplements the current upkeep surroundings, then this will be in line with the project or bring down the priority of that specific project.

Requirement as input for the framework:

No.	Category	Requirement
V3	Category	Project partitioning in different categories for business objectives, upkeep to stay secure, and resilience to continue to improve cybersecurity against changing cyber threats

The V3 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

Categorization is a useful way to organize. Projects can normally be categorized on the basis of budget, customer, and size, where size can be then classified into large or small projects. For this cybersecurity program, the categorization will be business objective, upkeep, and resilience. Categorization has different functions. First of all, categories serve as filters, allowing projects to be seen and discussed. A project can be seen and discussed with regard to many characteristics, such as size, budget, client, stakeholders, and so on. During categorization, only the relevant characteristics of a project are selected. Second, categories provide a priority selection. Hereby, they give an indication of the main focus points, in this case cybersecurity support, business objective, upkeep, and resilience (Crawford, Hobbs, & Turner, 2005).

Categorizing can be developed much further, for example into short-, medium-, and long-term projects, cybersecurity project development, or other ways of categorizing a project based on different objectives and features, to successfully run projects within organizations. Sauser, Reilly, and Shenhar conducted important research on the root cause of project failures. Failure in many cases is not technical, but managerial. Often the problem is rooted in management's failure to select the right approach to the specific project (Sauser, Reilly, & Shenhar, 2009). The authors have conducted important research regarding the categorization of projects. This thesis will describe only the cybersecurity categories that are most important for a common cybersecurity program. Other categories are more organization-specific.

Categories

Business objectives. There are several of projects that directly contribute to business objectives. It may be that there are projects from the business that work together with third parties, for example new software applications or cloud services to achieve greater efficiency. The cybersecurity projects in this category contribute to the business objectives; these are separate from the protection of the current environment, or they stay ahead of new threats, such as upkeep and Cyber resilience. There are different ways to identify these business projects; one of the best practices is clearly described in the book "Beyond Cybersecurity" (McKinsey, 2015).

Upkeep. This is the process of keeping something in good condition. Who will be responsible for the upkeep and the securing of the current ICT environment (oxforddictionaries.com, 2016b). Upkeep will focus on direct improvement of the current ICT cybersecurity situation. Investments are mostly prompted by "good house fatherhood" (taking good care of property) to stay secure by mitigating vulnerabilities, and they can also be triggered by savings due to high maintenance fees. An example of an upkeep project is the replacement of end-of-life firewall or proxy.

Cyber resilience. Resilience is the capacity to recover quickly from difficulties (oxforddictionaries.com, n.d.). The European Network and Information Security Agency (ENISA) argues that at the organizational level, resilience an additional dimension of a holistic strategic approach, with the result that the organization gains a new capacity to deal with different, even sudden and extreme shocks. (ENISA, 2010, p. 13) Understanding today's threats and attacks requires a different organizational understanding of cyber threats and the commitment to enclose protection, prevention, response, and recovery arrangements in the face of cyber-attacks to create cyber resilience.

Cyber resilience requires a holistic and complex combination of system hardening, system defense, access control, risk management, physical security, procurement control, internal and external monitoring, and cybersecurity training. Many of these already form part of the ordinary, or routine, organizational activities. The challenge is to know what an organization has, what it needs, and how to bridge the gap between the two in a dynamic threat landscape using the best practices within risk framework V1. The gap analysis is the key topic of this cyber resilience category (Ferdinand, 2015).

Importance of control

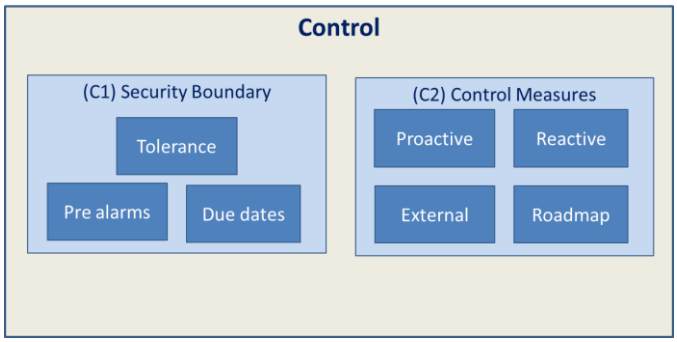

Figure 19. Framework program control methods

The main objective is to achieve the organization's goals by protecting what is most important for the business. Within different topics, this is elaborated with regard to how this must be done and how to organize the gaps. By mitigating the gaps to implement key cybersecurity projects and to control the timely implementation. This section of control will be used if the project threatens to become misaligned with the board-agreed appointments to protect the organization. As shown in figure 19. The category project (cyber)security boundary (C1) helps to identify project misalignments with the cybersecurity program, and the cybersecurity project category control measures (C2) help the decision-making process to stay on track.

No.	Category	Requirement
C1	Cybersecurity boundary	Clear expectation about the organizational cybersecurity risk tolerance and appetite, the timeframe of projects, and the definition of proactive indicators of due date failures

The C1 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

Cybersecurity project boundaries are needed to protect the organization from potential cybersecurity incidents. Within the value part of this framework, projects are initiated and prioritized based on the cyber threats and risk. The projects with a high priority need to be implemented within a timeframe before the organization becomes vulnerable to cyber-attacks. The V2 KPI has to provide the project implementation schedule tolerance and due dates. This section on the cybersecurity boundary will provide the necessary information to the project board to make the right risk-managed decisions by using the countermeasures of C2.

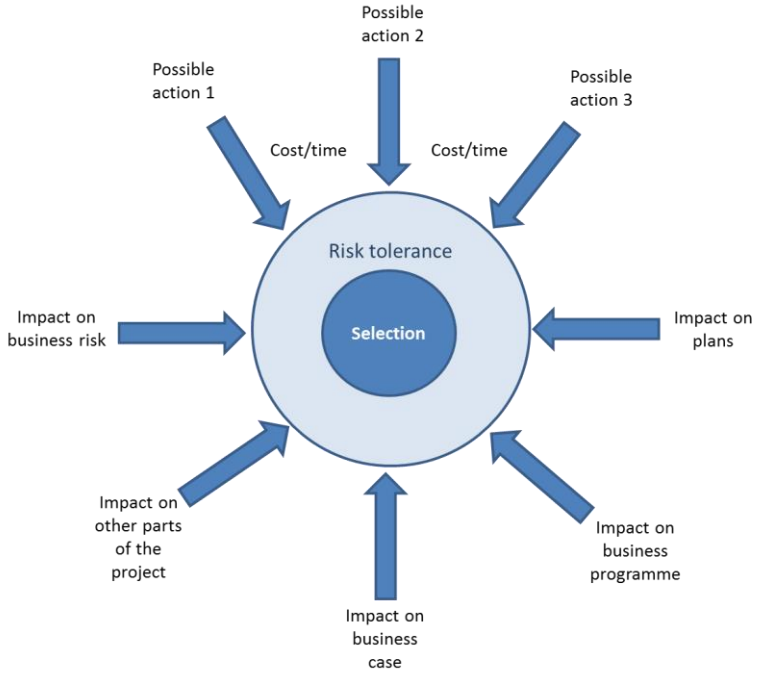

Figure 20. Risk action selection, Prince-2 (Fallis, 2013)

The risk action plan (Figure 20) provides the necessary information for the cybersecurity boundary to identify project tolerance risk and risk actions. In addition, project reporting by the project manager or project board must identify potential tolerance violations. The selection of the project risk actions to take requires a balance between a number of things. For each action, it is first a question of balancing cost of taken action against the likelihood and impact of allowing the risk to occur, as mentioned within KPI value V2. The selection is more complex; as figure 20 shows, there are many elements to take into consideration. There may be several possible risk actions. The choice may be one of these options or a combination of two or more. Then we should consider the impact of the risk occurring and the risk action based on the following:

- Impact on business risk
- The team, stage, and/or project plans
- The business or program
- The business case
- Other parts of the project.

The consideration has to be taken in light of the risk tolerances (Fallis, 2013, p. 256).

The project tolerance, the necessary pre-alarms, and due dates are defined in the “Value” section.

Requirement as input for the framework:

No.	Category	Requirement
C2	Control measures	Proactive and reactive countermeasures for project boundary and due date failures.

The C2 requirement is used to develop framework topics by using best practices from scientific research, analyzing literature, field experience and personal problem solving capabilities.

Ruling the program or project has everything to do with decisions, and decision-making falls within the program or project management. The projects need to be controlled to ensure that the desired result is delivered to the organization on time and within budget to manage risk. This control is also necessary to ensure that there is a valid business case to proceed with the project. For cybersecurity

projects, this not much different from normal projects or programs. The same methods can be used to steer. For this part, the best practice of the Prince-2 methodology for managing projects is used. The big difference between a normal project or a cybersecurity project is, in particular, the risk to which the organization is exposed within the cybersecurity domain, as well as the diversity of cybersecurity resilience in areas of projects needed to avoid incidents.

Control includes all steering and regulating activities aimed at ensuring that all specialists work according to plan. In contrast to the specialist activities, controlling is a continuously recurring process. Controlling is done as if it were in a "loop" of planning, recording, evaluating, and adjusting. The program manager is responsible for the management of the program, the project manager is responsible for the management of the project, and the team manager is responsible for the control of the work package.

By mastering the specific cybersecurity project, the organizational risk is safeguarded when every decision-maker stakeholder (team manager, project manager, Steering Committee, etc.) is involved and can assess the progress. The delivered results can be compared to the planned results, follow-up plans and options can be tested on several scenarios, problems can be detected, corrective measures can be taken, and the follow-up work can be authorized.

To master the program or project, a common method is to use management, except for senior management. This means that the project manager only reports to the members of the steering committee when needed from the management point of view. In addition, the report is focused on the management question of the business case or business-facing risk.

Control measures of the project board/steering committee

The most important countermeasures of the project board are the following:

- *The authorization to initiate and to start the project*. Is there enough reason to start the project? When is the budget approved to start the project?
- *Main reporting*. Interim reporting to the steering committee members to inform them about the progress of the project.
- *Exception report.* Reporting to the steering committee if the project manager finds that one or more tolerances of the project plan or program is/are likely to be exceeded.
- *Project closure*. This is the final steering committee meeting in which the members should be convinced that the project result was completed to the satisfaction of the different parties, that any follow-up actions are recorded, and that a good project and cybersecurity evaluation has taken place.
- *External influence.* This comes from a regulated body. Government, law, or customer contract can demand that a project be done within a timeframe.

To master the program or project, attention should be given to a controlled start, execution, and closing of the project.

Project tolerances

An important management tool is the match of tolerances and escalation processes. A tolerance is a permissible deviation from the agreed value, without requiring direct escalation to the next management level. Tolerances are necessary for small setbacks in the project implementation, and from the business risk point of view they control the timely completion of the project.

Tolerances must be agreed upon between the board-level program management and the steering committee, between the steering committee and the project manager, and between the project manager and the team manager, as shown in figure 21. This must be formally tracked.

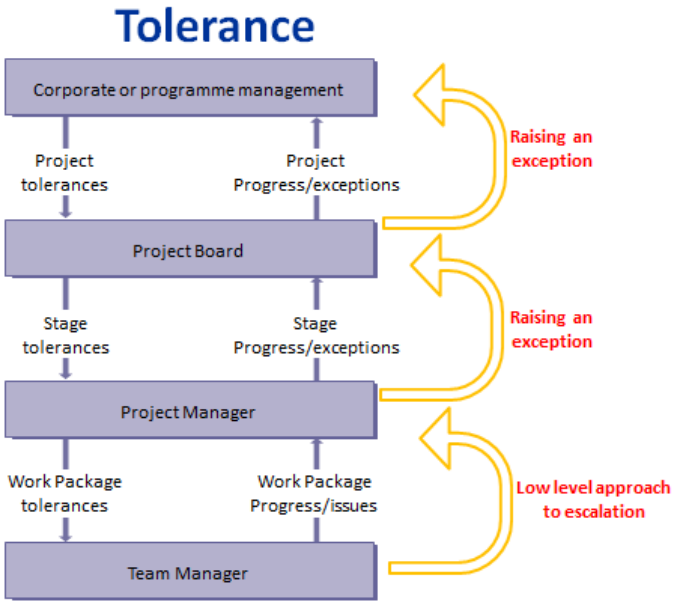

Figure 21. Prince 2 project tolerance (Stratsure, 2016)

For the tolerances, the Prince-2 best practice is also used as guide. Tolerances in projects are usually traditional agreements regarding time and money, but appointments regarding tolerances within the cybersecurity project domain may be different because of the aggressive cyber threats that are translated into business risk. The following are examples of tolerances:

- *Tolerances on risk.* How much risk is the steering group or board willing to take? Depending on the situation, for example, more risk can be taken regarding money than regarding time or quality for a direct cybersecurity threat.
- *Tolerances on added value.* If the cyber threat or risk profile does not change, the business case and priority stay current.
- *Tolerances on legal or external constraints.*
- *Tolerances on scope.* Internal scope changes for specific project topics to be accomplished or added. External scope changes because of business demand or changing threat level.
- *Tolerances on quality.* Desired properties of a particular product that determine what is and is not strictly necessary.

For tolerances regarding both time and money, there is an upper limit as well as a lower limit. Being too late or too early can lead to problems in coordination with other projects, or even to corporate risk due to increasing cyber threat or vulnerability.

Summary

In this section, three key attention areas the pillars of the decision support framework have been developed based on research, analysis of best practices and frameworks, and brainstorming. The first area is governance, which concerns successfully governing the cybersecurity program and influencing the key stakeholders. Governance covers the project's steering/control, the board-level dashboard, and KPIs for decision-making. The second area is value, where the cybersecurity analysis is conducted to initiate cybersecurity projects and to define KPIs and risk as input for the steering committees and governance category. In addition, projects are divided into categories, such as cybersecurity projects, to meet organizational objectives, such as new business services, protecting the current business ICT environment, or to update protection against new threats. The third area is control. Control is used when KPIs are triggered on the governance dashboard, in order to take action against the potential organizational risk. The framework consists of several steps to identify threats and risk, and to control

the needed safeguarded cybersecurity activities or projects outside ICT. The best approach to control this framework at different organizational levels as ICT department level, business level and executive boardlevel. The main reason is that cybersecurity risk is an organizational risk, and therefore has to be controlled by the executive board as strategic risk.

7.4 Implementing the decision support framework

To successfully implement the decision support framework for CISO, there needs to be guidance to successfully change the organization, and to embed cybersecurity within the current governance structure. From the literature review and the above summary, several best practices are identified to successfully govern the framework. The identified best practices in this topic are different than those described as IoT best practices. Within this topic the best practices are focused on successful implementing the cyber cybersecurity decision support framework. The four steps to prepare for successful implementation of forward change are the following:

Step 1 Create optimal governance to forward the needed change

Optimal governance with Silent Killer for change (Beer & Eisenstat, 2008). The Silent Killer for change practice divines solutions that are based on common practices that lead to organizational change failure. The optimal boundary conditions to successful implement the new framework can be created using the Silent Killers for change best practice method to successful implement the change strategy of the new decision support framework. What does it take to successfully implement a strategic plan? From an employee perspective, it requires leadership, teamwork, and strategic direction. Michael Beer and Russel A. Eisentat found this, and based on profiling organizations and detailed analysis, they identified six "silent killers" of strategy implementation. On the other hand, are success factors put down as core capabilities. The six core capabilities that are needed are:

1. A leadership style that embraces the paradox of top-down direction and upward influence
2. Clear strategy, clear priorities
3. An effective top team, whose members process a general management orientation
4. Open vertical communication
5. Effective coordination
6. Down-the-line leadership

In summary, for successful implementation of strategies, leadership should set direction, delegate authority for specific projects, and hold implementation teams accountable (Beer & Eisenstat, 2008). These capabilities should be taken into account when deploying the new cybersecurity framework or strategy. More information on the Silent Killers for change strategy is described in Appendix D, "The four steps of successful governance change."

Step 2 Specify the important stakeholders

The Power vs. Interest Matrix (Mendelow, 1991a) is a practice to identify key stakeholders, who has power to make decisions, and how to approach the stakeholders attention based at the level of cybersecurity interest. The practice supports the framework in being effective and successful within the steering committee or at the board level. Stakeholders are plotted in this matrix (see Figure 22) and the matrix can be used to determine the potential influence of stakeholders (or stakeholder groups).

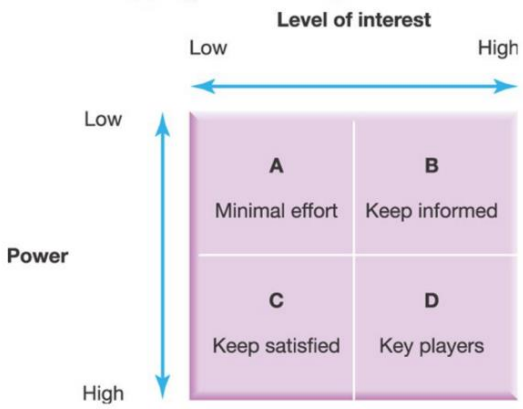

Figure 22. Stakeholder mapping: the Power vs. Interest Matrix. (Mendelow, 1991b)

The Mendelow Matrix is a useful matrix for determining the potential influence of the stakeholder groups of an organization. It looks at two dimensions: the level of interest that the group has in the organization, and the level of power or influence that it has over the organization. Power can be defined in many ways by the organization, from expertise in an area that fits with the organization's needs, to simply having a strong network of connections to which the organization requires access. More detailed information is described in Appendix D, "The four steps of successful governance change." The decision support framework contains "sense making" for influencing the different individual stakeholders.

Step 3 Create joint identity of the organizational cyber risk appetite

This best practice has the goal to create a joint identity of the given subject, and supports implementing the cybersecurity change for the decision support framework. This is a requirement to manage stakeholders within a complex cybersecurity environment, such as the (cyber) program or steering committee. "Wicked problems" (Camillus, 2008) often crop up when organizations have to face constant change or unprecedented challenges. The wicked problems are difficult or impossible to solve because of complex interdependencies. Solving one problem may create other problems. Wicked problems often arise when organizations have to face constant change or unprecedented challenges. Cybersecurity and IoT are hard and complex for different stakeholders to understand; Implementing changes to the organizational environment and processes, calls on the social context within the steering committee and possible disagreement between different stakeholders' own objectives. It is the social complexity of wicked problems as much as their technical difficulties that make them tough to manage. Rittel and Webber identified ten characteristics of a wicked problem, and defined five ways to manage these wicked problems. Appendix D describes these characteristics and management of the wicked problem. The five ways to manage them are summarized below:

- Involve stakeholders, document opinions, and communicate. The aim should be to create a shared understanding of the problem and foster a joint commitment to possible ways of resolving the problem.
- Define the corporate identity. It must stay true to a sense of purpose.
- Focus on action that one is willing to take.
- Adopt a "feed-forward" orientation. Take unusual steps to move forward instead of the well-known roads.

Step 4 Basic Program Management Platform

Portfolio Management (Fallis, 2013) is a best practice to manage multiple projects, in this case a cybersecurity project within an ICT department, at the business or board level. Portfolio management can also be called program management. Portfolio management includes managing a group of projects

and programs that bring together the new capabilities needed for one or more common business objectives. Portfolio management is the responsibility of the organizational management.

Portfolio management is there to realize the business objectives, and to implement the necessary improvements and the available deployment of people and resources. Portfolio management is used in the prioritization of the projects within the portfolio and the projects in relation to each other as project sequence and dependency of shared resources. The different projects sometimes jointly or separately deliver results in line with the objectives, or provide added value for an organization. Portfolio management does not realize the added value in portfolio management; this is done at a lower level program management, but portfolio management is only for the delivery of the various projects in relation to each other (VHP, 2005, p. 169). More detailed information on portfolio risk is described in Appendix D, "The four steps of successful governance change."

Cybersecurity project categorizing

An optimal and balanced mix of projects is one of the requirements for a cybersecurity project portfolio. To compare and prioritize projects, it is necessary and helpful to differentiate the projects. Project categorization is the method used to achieve this differentiation. In addition, these categories help decision-makers to understand to which organizational objective or risk the project contributes. For the decision support framework, specific categories were created by the brainstorming team: business objectives, upkeep, and resilience. The first aims to further help the business aims with new additions or improvements to the ICT facilities; the second regards the secure maintenance of the existing situation; and the third aims to remain resilient against new threats. These categories are

7.5 Summary

The development of the decision support framework is based on several requirements resulting from scientific research into literature, brainstorming, and interviews. The main task of the framework is to govern cybersecurity activities as strategic organizational value through the organization by identifying the main contribution to the organization's value of information assets and risk. It also aims to involve key stakeholders to manage the risk as strategic organizational risk within the executive board. Managing is done not with technical knowledge, but with business-understandable language and, if needed, strategic controls as corrective measures if deadline boundaries are in danger. This framework is a three-pillar model that gives guidance for strategic cybersecurity management to executive, business, and CISO stakeholders.

For the CISO, there is a four-step guide to implementing the framework as well as guidance for each applicable subject of decision support framework. The developed framework accomplishes the research goal: "To develop an (IoT) management decision support framework to safeguard businesses in a timely manner before possibly high-impact cybersecurity incidents become a reality." The framework is suitable for IoT management as well traditional ICT cybersecurity management. The management of projects at the strategic level is equal in both cases; only protective technical measures are different.

8 Validating the management decision support framework

Within this chapter the research sub-question “Is the developed framework useful for large organizations?” will be discussed. Validating the management decision support framework will prove the practical guidance of the proposed framework. A nearly authentic fictive case study was used from within the CISO field. The results should indicate whether the research goal has been met and whether or not the framework guide is practical and understandable for management. Moreover, this section discusses the pros and cons of the use case.

Fictional Case

Organization

The organization Zero Trust is a heat, ventilation and air conditioning (HVAC) supplier for critical infrastructures (CI). Critical infrastructures (Dutch: Vitale Infrastructuur) refers to products, services and the accompanying processes that, in the event of disruption or failure, could cause major social disturbance at national and international level (BZK, 2005). Thus, the CI supplier is crucial for ensuring the proper functioning of the CI. HVAC systems are high tech and remotely managed by their supplier. Using IoT innovation, customers of CI can remotely observe the environmental benefits of the systems since they lower environmental pollution. Zero Trust is a medium size enterprise with 600 employees, including the core executive board members: CEO, CFO and Business Unit (BU) directors.

Important assets

The organization Zero Trust stores important customer information, i.e. information regarding the precise, custom-made HVAC systems to support the CI systems. It is necessary to record this information because, for example, extreme temperature variations can significantly impact these CI systems, causing the systems to explode. Moreover, the HVAC techniques that this organization uses are quite unique within the CI industry, making it important that Zero Trust ensures the cybersecurity of their intellectual property.

ICT environment

Figure 23. HVAC IoT connected(blueapp, 2015)

The CIO reports to the CFO. The Zero Trust organization is connected to the internet so that it can remotely support its customers using IoT, as shown in figure 23. This IoT connection is additionally used to provide an overview of the HVAC’s economic benefits to the customer on their customer dashboard. Zero Trust also hosts a public website. Thus, it is important for the organization to act at a high cybersecurity maturity level within the ICT and development departments for the HVAC systems. The ICT environment is built on the basis of best practices and the NIST Cybersecurity framework (NIST, 2014a) for CI.

Cybersecurity organization

The organization has its own CISO who reports to the CIO. Once each year, the organization's board conducts a cybersecurity risk assessment. Projects are managed and integrated within the ICT department. The importance of cybersecurity is understood by all of the organization's employees. However, a majority of the organization's management failed a simple phishing test. Zero Trust's cybersecurity budget is 6-10% of ICT department's annual budget.

ICT department

The ICT department is well organized with ITIL (Cartlidge, Hanna, Rudd, Ivor & Stuart, 2007) processes and project program management. The ICT department supports new products and custom-made ICT environments for specific customers. The ICT department's objective is to be more efficient with short-time delivery and a target cost reduction of 10%.

ICT program management

The project steering committee is organized within the ICT department and the main stakeholders are the CIO, project management managers, the engineering and infra-structure manager, business application manager and the CISO. All projects are categorized as business, infra or cybersecurity projects, and are prioritized according to the needs of every stakeholder.

The business determines a yearly budget and roadmap to be followed; Each quarter the business meets to ensure that the organization is aligned with the project status. Stakeholders include the business representatives of business units, the CIO, Project management and the business application manager.

8.1 Methods used

To validate the management decision's support framework, a fictional case was used to test the framework's usability. The framework should provide practical guidance to the CISO so that he can govern the framework processes within the organization and provide key performance indicators to management to help them make a well-considered decision. The case study must prove the practical guidance of the framework.

8.2 Results of case study

The decision support framework consists of the "CISO Governance Program" and the "Cyber Resilience Program," as displayed in figure 24. The governance and resilience programs are dependent upon one another. The CISO Governance Program implements steering committees within the organization and the Cyber Resilience Program manages the cybersecurity project portfolio based on organizational risk and impact.

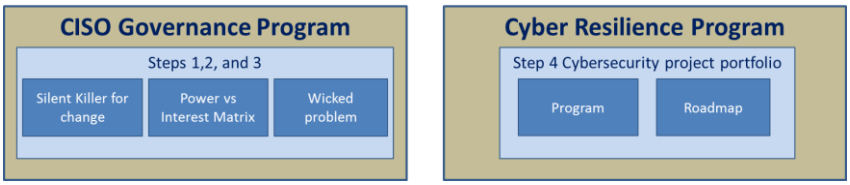

Figure 24. Four steps implementation of management decision support program.

CISO Governance Program

Through the governance and resilience programs, the CISO supports all of the key stakeholders in running the cybersecurity program. The CISO uses steps 1, 2, 3, and 4. to govern the management decision support framework within the organization.

Step 1: Create optimal governance for forwarding the needed change. The CISO uses this step to prepare and influence stakeholders using the top-down, upwards influence, determine which

stakeholders and steering committees are needed (depending on the organization's size and hierarchy) and communicate and coordinate with best practice methods to deliver the messages that influences cybersecurity awareness.

Step 2: Specify the important stakeholders. This step determines which key stakeholder is needed within the steering committee and who is influencing the key stakeholders. Determine the needed key stakeholders for the steering committee, how much influence power do they have, what is their interest in the cybersecurity topic and does he/she uses other for him trustable stakeholders to inform himself about this cybersecurity topic. Based on an analysis of the stakeholders and their influence over organizational power and interest, key stakeholders are informed via a custom-made awareness message.

Step 3: Create joint identity. Involve stakeholders using steps 1 and 2 and create a shared understanding of the importance of cybersecurity within the organization. Creating a trusting image for the corporation's identity, in this case Zero Trust, is a core organizational value.

Step 4: Basic program management platform. Create a cybersecurity program and roadmap to mitigate threats to cybersecurity based on the framework for identifying cybersecurity threats. Step 4 uses steps 1, 2 and 3 to create steering committees (together with the G1 step of the framework) within the organization at different levels. In this case, there is a cybersecurity steering committee at the executive board level that will update the cybersecurity program's dashboard quarterly. A monthly cybersecurity steering committee occurs at the business level; The members are business unit, human resource, Legal, Facility, ICT and CISO directors or representative members. The same steering committee used in the ICT department for ICT projects is also used for the cybersecurity projects. Major decisions are made at the BU level and strategic decisions are made at the board level.

The cybersecurity governance program is a continues process that is necessary for the adequate governance of the framework and cybersecurity program.

Results of CISO Governance Program

The result of this program is the creation of steering committees at the executive board level, business level and ICT department level. Important stakeholders have the importance of the organization's cybersecurity explained to them individually and all of the members of the steering committees have the same corporate identity within the cybersecurity program.

Cyber Resilience Program

The Cyber Resilience Program consists of three main pillars, as depicted in figure 3: Pillar GOVERNANCE for steering the cybersecurity portfolio, VALUE for defining the projects within the portfolio and its importance to the organization based on risk and CONTROL for the timely implementation of cybersecurity projects.

Step 1 VALUE

Value V1 identifies an organizational cybersecurity risk and its impact on the organization based on analysis, compliance and best practices.

Example case: The identified organizational risk will significantly impact the organization's reputation: Company and customer secrets may be stolen and normal operations may be disrupted in case of a zero-day attack (FireEye, 2015) through the use of command and control malware that can

bypass the normal virus scanner in the e-mail server. Thus, the organization should implement sandbox capabilities that can identify zero-day malware by testing the attachments within e-mails. Therefore, the firewall needs to be replaced with new sandbox features.

Value V2 and V3 prepare the steering committees' key performance indicator (KPI). The KPI may comprise organizational risk, the priority and type of project for business, ICT upkeep or resilience to new threats, and the cybersecurity project implementation deadline.

Example case: It is crucial to determine the protect priority for the resilience (Moscow MUST type) of the organization based on the V1 risk assessment. The project needs to be implemented by the end of March of the subsequent year. The project implementation time is eight weeks.

Step 2 GOVERNANCE

In governance G1, G3 and G4, the steering committee is defined with all aspects of the budget, organizational value and organizational cybersecurity risk appetite as defined within the framework. Specific cybersecurity awareness is presented to its stakeholders and all of the cybersecurity projects are translated into organizational risk.

Example case: In this example, the organizational cybersecurity risk appetite is minimum.

Governance G2: The executive board's dashboard consists of the key cybersecurity project KPI with organizational risk and deadlines for the project. However, the business steering committee does have a more detailed KPI dashboard of the portfolio with organizational risk, deadline (due date) and planning tolerance indicators. The steering committee of the ICT department consists of the ICT portfolio with the due dates, priority and sequence of the cybersecurity projects.

Example case: The ICT department has a considerable backlog of up-keep activities and the ICT operation has network performance issues. The previous year's network replacement project was delayed by its complexity and availability of resources within the network team. The same network team manages the organization's firewalls. The ICT steering committee decided that due to the needs of the business, the network project needs to be finalized before running the firewall replacement project. It has been estimated that the network project requires four weeks to finalize. The firewall replacement project has to move four weeks. Reasons for the ICT department to not escalate the postpone of the firewall project is that there is no direct cybersecurity problem, and for the ICT department the network project is really important. Postpone the firewall project a couple of weeks must not be a problem. Everyone agreed except for the CISO.

The business steering committee meets monthly. The first meeting is on the first of January. The dashboard indicates the project's firewall replacement start date and the CISO reports the four week delay. The project risk KPI exhibits a high risk if this project is not implemented. Subsequently, the CONTROL pillar is activated.

Step 3 CONTROL

Control C1 feeds the steering dashboard with the KPI cybersecurity boundaries, risk, impact on plans, other cybersecurity projects and possible actions.

Example case: The dashboard revealed that project tolerance was two weeks. The project needed to start in February and a delay of four weeks was not acceptable to the organizational risk or the cybersecurity project's boundary. Additionally, the steering committee had the mandate, given the organization's cybersecurity risk appetite , to begin remediation actions. Action plan 1 (part of C2) was activated to deploy the external supplier's consultant for the firewall, who was already familiar

with the organization's ICT environment. The consultant implemented the firewall without the ICT network team. The steering committee reported the action to the CIO and to the executive steering committee board. The executive steering committee was pre-informed about the actions and did not have to escalate, only exceeding the budget could affect the ICT budget. The CFO decided what the follow-up action should be of the budget exceedance.

Two months later, the organization was attacked by zero-day malware but this was not effective because of the new firewall.

8.3 Evaluation

The use case exhibits the function of the cybersecurity management's decision to support the framework. The research goal *"To develop an (IoT) management decision support framework to safeguard businesses timely before possibly high-impact cybersecurity incidents become a reality"* was achieved through this use case.

Pros

- The framework is designed to place the decision-making process at the correct organizational level as business level or executive board.
- The framework is designed to translate cybersecurity threats into organizational risk.
- Cybersecurity risks are strategic risks and as such, need to be handled at the strategic level. The ICT department's priorities or the day-to-day activities at a lower organizational level cannot influence the organizational risk. The framework supports the CISO to impose risk responsibility at the appropriate level.

Cons

- The success of the framework depends on the CISO understanding the capabilities for translating cybersecurity projects into organizational risk. Moreover, since a technical risk analysis is performed by the CISO, the right education and expertise levels are important. Otherwise, a not trained CISO can be an organizational risk if threats are not detected.
- The framework informs the business and board about the autonomy of the ICT department, its performance and the consequence of allowing it controlling its own projects. This can either be negative for the department's reputation or positively help ICT to increase the cybersecurity budget and resources.
- While this use case is fictional, it could be a real scenario. Also other use-cases need to be tested. Testing in practice will prove the framework's real capabilities.

8.4 Summary

With this use case, the function proof for the decision support framework is displayed. The research goal *"To develop an (IoT) management decision support framework to safeguard businesses timely before possibly high-impact cybersecurity incidents will become a reality"* can be achieved by implementing this framework. Additionally, this framework helps the executive board and business understand what are the cybersecurity organizational risk contents as well as the importance of cybersecurity spending. However, the success of this framework does depend on the CISO's skills and knowledge.

9 Conclusion and discussion

This chapter discusses the main conclusions and contributions of this thesis, as well as recommendations, limitations, and further research possibilities.

9.1 Conclusions

The management decision support framework is a generally applicable methodology for reasoning about cybersecurity project priorities. It is especially well suited to stakeholders of cybersecurity steering committees and decisions makers. The complex cybersecurity language will be translated with the help of the framework into business language. Several sources have shown that past cybersecurity incidents would have been preventable if the right cybersecurity measures had been implemented. Analyzing cyber threats and risk, and translating them into projects and portfolios will help organizations to protect themselves. This framework will support organizations to control cybersecurity project implementations by focusing on three key attention areas. The first one is governance, for controlling and understanding cybersecurity as a strategic topic throughout the whole organization. The second is value, to identify the cybersecurity project's value for the organization, and to protect what is important or to gain business benefits. The third key attention area is control. Controlling what was agreed in advance will ensure that it is fulfilled and not ignored in favor of other competitive projects. Otherwise, this competition could impact the entire strategic cybersecurity roadmap and organization-facing risk.

9.2 Main contributions

The goal of this thesis was to build a decision support framework for management to support the latter with cybersecurity project priority decisions. This was done because cybersecurity is often handled within the ICT department, and within this department cybersecurity has to deal with competitive project priorities. This can be a major organizational risk if key cyber projects are delayed. The contributions of the decision support framework are aligned with the research sub-questions:

1) **What is IoT and why is cybersecurity so important?** IoT is a new innovative development in which ICT systems interconnect with each other. The prediction is that in the future IoT will be integrated within organizations; however, at the moment IoT systems are far from secure. Integrating these systems within current enterprise networks needs specific attention. Integrating IoT cybersecurity is even more important.
2) **What is the business impact and/or societal impact if IoT cybersecurity is not handled and prioritized as needed within organizations?** Organizations are fully dependent on ICT services and information assets. If there is a cybersecurity incident through IoT, for some organizations this can have a major impact on trust, reputation, and finances. It is a must to prioritize cybersecurity with the integration of IoT.
3) **Are existing cybersecurity projects handled in a timely way to reduce business impact between the competing priorities of ICT departments? What causes or blocks issues, and what are the best practices to solve these issues?** In the interviews, a few participants talked about projects that were not handled in a timely manner, and were postponed. Fortunately, this had no impact on the organization. Public cyber incidents, on the other hand, show that incidents could have been avoided if organizations had taken the right measures. Considering the cause of the incident, the interviewees, and my own experience, cybersecurity project prioritization and monitoring are often done within ICT and not at a strategic level within the organization. However, cybersecurity is a strategic issue. The best practices for prioritization and monitoring cybersecurity projects are outside of ICT. Because cybersecurity is a complex subject and difficult to understand, the framework developed in this thesis offers best practices to control successful roll-out of cybersecurity projects using best practices.

4) **Given the answers to the previous questions, what would a cybersecurity management decision support framework for large organizations look like?** The decision support framework has three key attention areas. The first is governance for controlling top-down cybersecurity projects within the organization. Within governance, the organizational risk appetite will be cleared, the steering committee will be arranged, there will be a KPI dashboard for controlling the projects, and special attention will be paid to all involved stakeholder awareness. The second key attention area is value. Within value, the projects are initiated by assessments and compliance, and cyber risk is translated into organizational risk and impact. In addition, the projects will be divided into different categories and priorities. There will be categories for different risk areas and organizational objectives, and priority will be given to what needs to be implemented first within a category. The third key attention area is control. If a project seems to be delayed or postponed, it will require strategic attention if the predefined boundaries are passed. The control takes care of the alarm and countermeasures to stay on track.
5) **Is the developed framework useful for large organizations?** The interviews showed that larger organizations are much more mature than other organizations with regard to cybersecurity project priority handling. However, cybersecurity projects are not structurally managed by the board. Moreover, these are often only concerned with escalations. The proposed framework will certainly help larger organizations to better manage cybersecurity projects, and will help board members to better understand the risk and how the organization is protected against that risk.

9.3 Additional insight

This thesis has shown that there are many best practices and frameworks for cybersecurity, but they give no guidance to control effective project implementations. What also emerged from the research is that the degree of protection within many organizations depends on the commitment and expertise of the cybersecurity expert. The interviews showed that the cybersecurity representative level of knowledge or reference framework is not always equally good. This can have a big impact on an organization.

9.4 Thesis limitations

This is a highly explorative research. Due to the practical limitations of this thesis, not all best cybersecurity practices and countermeasures could be integrated. However, the framework is set up to use practices that best fit the organization itself. It offers practical guidance. It was not feasible to take into account new or additional working methods, such as agile/scrum methods. There was limited time to interview the respondents, which meant that not all questions were very deeply discussed. Still, an overall view of the cybersecurity practice within the interviewees organization was created with regard to managing and controlling key cybersecurity projects within the organizations, and how to involve and inform key stakeholders. To validate the framework and principles and to ensure that they are effective and complete, further research is needed, in which more respondents could also be interviewed.

9.5 Future research possibilities

It was interesting to build this framework; it gives the possibility to use best practices for developing the framework. Further development possibilities could be the integration of other cybersecurity activities and projects – for example, the integration of audits, awareness, and repetitive tasks such as patching, and the KPI dashboard for the board. In addition, specific framework aspects could also be integrated, such as ISF Standard of Good Practice maturity levels. The board would then be able to control based at desired maturity levels.

Bibliography

Agilebusiness. (2008). MoSCoW Prioritisation | Agile Business Consortium. Retrieved December 23, 2016, from https://www.agilebusiness.org/content/moscow-prioritisation-0

April, A., Hayes, J. H., Abran, A., & Dumke, R. (2005). Software Maintenance Maturity Model (SMmm): The software maintenance process model. *Journal of Software Maintenance and Evolution*, *17*(3), 197–223. http://doi.org/10.1002/smr.311

Beer, & Eisenstat. (2008). The Silent Killers of Strategy Implementation and Learning. Retrieved November 24, 2016, from http://www.opia.psu.edu/extracts/silent-killers

Belden. (2016). Belden and Weidmüller Present Modular Infrastructure Box. Retrieved January 9, 2017, from http://www.machinebuilding.net/p/p7848.htm

Belden. (2016). IIoT Example. Retrieved January 9, 2017, from http://www.belden.com/blog/industrialsecurity/images/IIoT-Mobile-Applicaions-LG.jpg

Belden. (2016). The IIoT Journey – with 4 Examples of Today's Solutions. Retrieved January 9, 2017, from http://www.belden.com/blog/industrialethernet/The-IIoT-Journey-with-4-Examples-of-Today-s-Solutions.cfm

blueapp. (2015). HVAC IoT example. Retrieved January 21, 2017, from http://blueapp.io/wp-content/uploads/2015/07/HVAC-1-1024x598.jpg

businessdictionary.com. (2016). What is a steering committee? definition and meaning - BusinessDictionary.com. Retrieved January 10, 2017, from http://www.businessdictionary.com/definition/steering-committee.html

BZK. (2005). Rapport bescherming vitale infrastructuur, (september), 1–69.

Cambridge. (2016). mandate Meaning in the Cambridge English Dictionary. Retrieved December 10, 2016, from http://dictionary.cambridge.org/dictionary/english/mandate

Camillus, J. C. (2008). Strategy as a wicked problem. *Harvard Business Review*, *86*(5). http://doi.org/Article

Cartlidge, A., Hanna, A., Rudd, C., Ivor, M., & Stuart, R. (2007). *An introductory overview of ITIL V3*. *The UK Chapter of the itSMF*. http://doi.org/10.1080/13642818708208530

Castellote, G. P.-, & Ph, D. (2015). Securing the IIoT with DDS- - - Security The Industrial Internet of Things, (June).

CMMI. (2013). Security by Design with CMMI for Development, Version 1.3: An Application Guide for Improving Processes for Secure Products, (May), 1–80. Retrieved from http://cmmiinstitute.com/sites/default/files/resource_asset/Security-by-Design-with-CMMI-for-Development V1.3.pdf

Crawford, L., Hobbs, J. B., & Turner, J. R. (2005). *Project Categorization Systems: Aligning Capability with Strategy for Better Results*. *Project Management Institute* (Vol. 37). http://doi.org/10.1145/363332.363339

DNS. (2015). INTERNATIONAL ATOMIC ENERGY AGENCY Nuclear Security Series Glossary, *1.3*.

Drake, J., & Byrd, T. (2006). Risk in I Nformation T Echnology Project. *Journal of Information Technology*, *8*(3), 1–11.

Economist, T., Unit, I., & Enterprise, H. P. (2016). Securing the internet of things The conversation every CIO needs to have with the CEO, 1–5.

en.oxforddictionaries.com. (2016). compete - definition of compete in English | Oxford Dictionaries. Retrieved December 28, 2016, from https://en.oxforddictionaries.com/definition/compete

en.oxforddictionaries.com. (2016). framework - definition of framework in English | Oxford Dictionaries. Retrieved December 28, 2016, from https://en.oxforddictionaries.com/definition/framework

en.oxforddictionaries.com. (2016). management - definition of management in English | Oxford Dictionaries. Retrieved December 28, 2016, from https://en.oxforddictionaries.com/definition/management

en.oxforddictionaries.com. (2016). priority - definition of priority in English | Oxford Dictionaries. Retrieved December 28, 2016, from https://en.oxforddictionaries.com/definition/priority

en.oxforddictionaries.com. (2016). support - definition of support in English | Oxford Dictionaries. Retrieved December 28, 2016, from https://en.oxforddictionaries.com/definition/support

ENISA. (2010). Enabling and managing end-to-end resilience.

Ernst & Young. (2014). Cyber program management every day .", (October).

Fallis, A. . (2013). Managing Successful Projects with PRINCE-2. *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. http://doi.org/10.1017/CBO9781107415324.004

Ferdinand, J. (2015). Building organisational cyber resilience : A strategic knowledge-based view of cyber security management, *9*(2), 185–195.

Ferrillo, P. A. (2014). Cybersecurity, Cyber Governance, and Cyber Insurance: What Every Director Needs to Know. *Corporate Governance Advisor*, *22*(5), 1–5. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=97611591&site=eds-live

FireEye. (2015). What is a Zero-Day Exploit | FireEye. Retrieved January 14, 2017, from https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Gartner. (2016). The Internet of Things - Internet of Things Companies. Retrieved October 14, 2016, from http://www.gartner.com/it-glossary/internet-of-things/

Greenough, J., & Camhi, J. (2016). IoT next Industrial Revolution. Retrieved November 13, 2016, from http://www.businessinsider.com/iot-trends-will-shape-the-way-we-interact-2016-1?international=true&r=US&IR=T

Gregg, B. R. (2010). The CFO's Role in Managing Cyber Risk. *Financial Executive*, (september), 61–63.

Hevner, a. R., March, S. T., & Park, J. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. http://doi.org/10.2307/25148625

Hewlett Packard Enterprise. (2015). Internet of Things Research Study 2015 Report, (July), 4. Retrieved from http://fortifyprotect.com/HP_IoT_Research_Study.pdf

Homeland Security. (2016). STRATEGIC PRINCIPLES FOR SECURING IoT, 1–17.

Hornyak, T. (2015). Hack to cost Sony $35 million in IT repairs | CSO Online. Retrieved December 28, 2016, from http://www.csoonline.com/article/2879444/data-breach/hack-to-cost-sony-35-million-in-it-repairs.html

Hyde, J. (1999). Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations (4th edn) (Book). *Logistics & Transport Focus*, *1*(2), 67.

Industrial Internet Consortium. (2016). Industrial Internet of Things Volume G4 : Security Framework.

Internal affairs New Zealand. (2014). Risk Assessment Process, (February).

ISACA. (2015). Internet of Things: Risk and value considerations, (October), 1–13.

ISF. (2013). Information Security Forum (ISF), The Standard of Good Practice for Information Security, (July). Retrieved from https://www.securityforum.org/shop/p-71-173

ISF. (2014). Time to Grow Review and quality assurance, (September).

ISO/IEC. (2009). ISO31010, *2009*.

ISO/IEC. (2011). ISO27005, *2011*.

ISO/IEC. (2013a). ISO27000, *2013*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=42103

ISO/IEC. (2013b). ISO27001, *2013*. Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534

ITSMF. (2004). *IT Service Management een introductie*.

Jason D. Christopher. (2014). Cybersecurity Capability Maturity Model (C2M2). *Department of Homeland Security*, (February).

Kaspersky. (2015). The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide.

Korsten, A. F. A. (2003). Organiseren volgens Karl Weick - De sociale psychologie van organiseren.

KPMG Advisory. (2015). Cyber Security Dashboard.

KrebsOnSecurity.com. (2016). KrebsOnSecurity Hit With Record DDoS — Krebs on Security. Retrieved January 11, 2017, from https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

McKinsey. (2015). *Praise for Beyond Cybersecurity*.

Mendelow, A. (1991a). Stakeholder Mapping. *Proceedings of the 2nd International Conference on Information Systems, Cambridge, MA (Cited in Scholes, 1998)*.

Mendelow, A. (1991b). Stakeholder Mapping: Power/Interest Matrix. Retrieved January 10, 2017, from http://images.slideplayer.com/14/4205073/slides/slide_32.jpg

NCSC. (2011). DigiNotar | NCSC. Retrieved January 21, 2017, from https://www.ncsc.nl/actueel/dossiers/diginotar.html

NCSC. (2015). Cyber Security Assessment Netherlands 2015.

NCSC-NZ. (2013). CYBER SECURITY AND RISK MANAGEMENT An Executive level responsibility.

NIST. (2014a). NIST Cybersecurity Framework, *V1.1*. http://doi.org/10.1109/JPROC.2011.2165269

NIST. (2014b). Security and Privacy Controls for Federal Information Systems and Organizations

Security and Privacy Controls for Federal Information Systems and Organizations. *NIST SP 800-53R4*, 400+. http://doi.org/10.6028/NIST.SP.800-53Ar4

NIST. (2016a). About NIST | NIST. Retrieved January 21, 2017, from https://www.nist.gov/about-nist

NIST. (2016b). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *NIST SP 800-160*.

OnlineTrustAlliance. (2016). IoT Trust Framework®.

oxcomlearning.com. (2015). Stakeholder Mapping. Retrieved from http://www.oxcomlearning.com/pluginfile.php/.../Mendelow Matrix.pdf

oxforddictionaries.com. (n.d.). Resilience. Retrieved from The capacity to recover quickly from difficulties; toughness

oxforddictionaries.com. (2016a). safeguard - definition of safeguard in English | Oxford Dictionaries. Retrieved January 9, 2017, from https://en.oxforddictionaries.com/definition/safeguard

oxforddictionaries.com. (2016b). Upkeep. Retrieved December 27, 2016, from https://en.oxforddictionaries.com/definition/upkeep

PCM, & Hofmans, T. (2015). Hackers kraken slimme thermostaat NEST. Retrieved January 11, 2017, from http://www.pcmweb.nl/nieuws/hackers-kraken-slimme-thermostaat-nest.html

platform4.0. (2016). Plattform Industrie 4.0 - What is Industrie 4.0? Retrieved January 10, 2017, from http://www.plattform-i40.de/I40/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html;jsessionid=0E4BDDB1110DE8168112A0FAC6DC17D4

Post, D. (2014). Cybersecurity in the Boardroom: The New Reality for Directors. Retrieved January 12, 2017, from https://iapp.org/news/a/cybersecurity-in-the-boardroom-the-new-reality-for-directors/

PwC Nederland. (2014). Cyber Governance Onderzoek: Volwassenheid van cyber beheersing binnen Nederlandse organisaties.

SANS. (2015). Critical Controls that Sony Should Have Implemented. Retrieved from https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

SANS. (2016a). Critical Controls. Retrieved from https://www.sans.org/critical-security-controls/

SANS. (2016b). SANS IT Security Spending Trends. *Worm Propagation and Countermeasures*, 36.

Sauser, B. J., Reilly, R. R., & Shenhar, A. J. (2009). Why projects fail? How contingency theory can provide new insights - A comparative analysis of NASA's Mars Climate Orbiter loss. *International Journal of Project Management*, *27*(7), 665–679. http://doi.org/10.1016/j.ijproman.2009.01.004

security.nl. (2016a). Minister wil hack Nederlands-Duits defensiebedrijf niet bevestigen - Security.NL. Retrieved January 11, 2017, from https://www.security.nl/posting/476815/Minister+wil+hack+Nederlands-Duits+defensiebedrijf+niet+bevestigen

security.nl. (2016b). USB besmette Duitse kerncentrale. Retrieved November 13, 2016, from https://www.security.nl/posting/472938/Usb-stick+besmette+Duitse+kerncentrale+met+malware

Security of Things World USA. (2016). IoT World USA Survey report 2016.

Stratsure. (2016). Project tolerance. Retrieved from http://www.stratsure.co.za/sites/default/files/tolerances-graph.png

Ten, C.-W., Liu, C.-C., & Govindarasu, M. (2007). Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees. *2007 IEEE Power Engineering Society General Meeting*, *2*, 1–8. http://doi.org/10.1109/PES.2007.385876

Verizon. (2015). State of the Market The Internet of Things 2015, 1–24. Retrieved from http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf

VHP. (2005). *Projectmanagement op basis van Prince-2* (2e druk).

Weick, K. E. (1995). Sensemaking in Organizations (Foundations for Organizational Science). *Star*, 235. http://doi.org/10.1177/009539978601800106

Appendix A - Interview questions

Introduction

This questionnaire is part of my Master in Executive Cybersecurity at Leiden University. All replies to this interview are handled anonymously.

My thesis is about adequately protecting the business against cybersecurity risk, by ensuring that key cybersecurity activities are being executed within the organization. The goal of the thesis is to provide a decision support framework for management to manage key cybersecurity activities next to competing priorities of business and ICT. Doing by creating requirements, using interviewing cybersecurity experts about the priority control of key cybersecurity activities/measures and the impact if organizations do not implement the key cybersecurity measures in a timely manner. The thesis especially focuses on new innovations, such as the Internet of Things (IoT), where adequate protection is even more important because of weak cybersecurity and vulnerabilities.

IoT

IoT can be a powerful concept. IoT has the potential to be huge and is already changing the way people live, work, and play. Its advantages are numerous and can be efficiency (smart cities and industry 4.0), cost saving for businesses, life changing, and lifesaving.

The wave of changes from IoT also brings with it new and more complex risk and problems. With the adoption of any change, it is crucial to be well prepared. IoT can be a powerful concept, but making use of it responsibly requires forward thinking and appropriate planning (ISACA, 2015).

If the integration of IoT within organizations becomes a reality, appropriate cybersecurity levels will become even more important to control the cybersecurity risk.

Governance

1. Can you describe the size of your organization, meaning the number of employees, whether it is nationally/internationally oriented, its business activities, and revenue?
2. Do you see a demand for IoT systems within your organization at this moment or in the future? Please explain, and if so, what is your opinion about the risk towards your organization? How will you mitigate these risks? And will this influence your current protection level? Will this demand also affect classified networks?
3. What is the percentage of the overall annual ICT budget for cybersecurity, and how is the budget spending divided between different cybersecurity categories (for example, technology, awareness, etc.)?
4. How do you involve the board of directors in the importance of cybersecurity? What is the mutual expectation, and what are the best practices to get board-level attention?
5. Does cybersecurity have a clear mandate on different levels within the organization? Are you able to overrule management priorities?
6. What kind of steering committees do you have for cybersecurity? What information does the steering committee or management team (MT) need to take adequate decisions regarding to priorities of cybersecurity implementations and activities?
7. What is the level of cybersecurity awareness and understanding among decision-makers relative to the importance of protecting the organizational interest or protecting it against threats? And are you able to overrule these decisions?

Value (risk/impact):

8. Are you familiar with the risk and threats that your organization is facing in the area of (cyber) security? Please elaborate on how you stay updated and controlled within this field (for example, critical updates, vulnerabilities, threat actors, etc.) (source: National Cybersecurity Assessment).
9. Are you able to comply with or implement all of the latest cybersecurity best practices, such as the SANS.ORG critical controls, within your organization? And are you able to comply with the latest regulated compliance requirements? If so, why are you implementing all controls? If not, why not, how come, and how much time is needed to do so? How do you know that the protection level is high enough?
10. If a cybersecurity incident impacts your organization important assets, how would you describe the impact and damage to your business, your customers, and if applicable the societal impact? Can you elaborate on the possible damage figures (for example, the Sony hack)?
11. What are the most important cybersecurity activities to protect your organization important assets (technical cybersecurity improvements, patching, vulnerability scanning, awareness, etc.)?
12. How does your organization handle significant risk that has seemed to exist for many years, but that has not yet been exploited?

Control (projects/improvements):

13. Does your organization have a cybersecurity roadmap with different projects? How do you know what kinds of projects are needed, and how are the projects prioritized? How do you determine the start date, and is the original start date executed and implemented in a timely manner as planned? If not, what are the most common reasons and what would be the best approach to accomplish your cybersecurity roadmap?
14. How do you determine the priority of project or activities (for example risk assessment regarding threats that are translated into projects)? If applicable, with whom do you align these priorities (for example, the steering committee) and how are they monitored, adjusted, or controlled? Can you describe the process?
15. Does your organization have a steering committee to follow and control cybersecurity implementations? Who is accountable and responsible? How do you control or prevent these projects from being delayed? Is there an escalation procedure to the board of directors, and if so how does this work?
16. How do you prioritize and control plannable cybersecurity activities, such as patching, cleaning firewall rules, audit admin accounts, etc., that are executed within your organization (for example, agreements with responsible teams/supplier)? And are these activities done according to a previously discussed timeframe?
17. Is the steering committee effective in treating all key cybersecurity activities with proper priority? If not, what kinds of activities (grouped)? And how do you secure these key activities on different organization layers (operational, tactical, and strategic)? Please briefly describe the structure or process (e.g. patching, project cybersecurity requirements met before production, etc.)?
18. According to a recent study, many organizations are struggling to implement cybersecurity projects and innovations because of different competing priorities within the ICT department. Do you have the same struggle? Please elaborate on your answer about the current state: what are the bottlenecks and what do you think will be the best way to solve this problem as common practice?

19. Has the risk or threat ever increased because cybersecurity activities or projects were not implemented in time? What is the average increased period in time (week, months) and could this/did this impact the organization (for example, the Sony hack)?
20. Say you are ready to implement an important cybersecurity project and the budget is allocated, but you are not able to implement the project due to another project or lack of available manpower/resources. How do you, or how does your organization, handle this issue? If not handling this issue, what would be the best way to handle this situation?
21. Is there anything that you would you like to add?
22. May I ask questions about the answers or ask additional questions?

Appendix B - Requirements from interviews

Figure 25 shows the summarized requirements from appendix F (the interview results). Based on the subject the requirements are categorized in different category requirements. These categories are used within the management decision support framework (Chapter 7).

Nr.	Topic	Category	Requirements
R19	Controls	Cybersecurity Boundary	Ensure that the mandate does not have to be required too much in advance. By having clear beforehand what the board level expectations are around implementing cybersecurity activities carried through the whole organization.
R32	Controls	Control measures	Senior management level. Set direction to ensure that resources are available to allow for prioritization of possible controls and countermeasures implement accordingly on a timely basis, and maintained effectively.
R33	Controls	Cybersecurity Boundary	Monitor and control cybersecurity project priority and due date.
R34	Controls	Control measures	Project priority control instruments
R35	Controls	Control measures	Controls for managing KPI
R36	Controls	Control measures	Resource cybersecurity knowledge and availability
R37	Controls	Control measures	(external consultancy, long term relation?)
R1	Governance	Dashboard KPI	A better overview of spending around cybersecurity and board level KPI for benchmark own cybersecurity budget spending compared to any other similar industry organizations as a performance indicator. For better understanding of prober cybersecurity spending alignment to facing risks.
R10	Governance	Steering Committee	Regularly align with stakeholders at different organizational levels.
R11	Governance	Stakeholder Awareness	Cybersecurity awareness of key stakeholders
R12	Governance	Steering Committee	Cybersecurity Steering committees at different organizational levels as ICT, business and board.
R13	Governance	Stakeholder Awareness	Right involvement of stakeholder and awareness
R14	Governance	Dashboard KPI	Cybersecurity operational KPI dashboard for steering committee of risk appetite and agreements.
R15	Governance	Dashboard KPI	Right balance for execution, dependency, resources and priorities between other programs and projects
R16	Governance	Stakeholder Awareness	Stakeholder cybersecurity awareness. In general and individual.
R17	Governance	Dashboard KPI	Boundary controls of cybersecurity projects to align with strategic organization objectives
R18	Governance	Cybersecurity Business Risk	Organizations has to be cyber resilient to adopt new technologies like IoT
R2	Governance	Stakeholder Awareness	Recurring board level involvement and understanding of cybersecurity issues related to organizational impact.
R3	Governance	Dashboard KPI	Insist that management makes cybersecurity investments and cybersecurity improvements measurable, and monitors and reports on program effectiveness
R4	Governance	Steering Committee	Set-up steering committees on the needed levels where different stakeholder as board, business, IT and operational implementation. They need be involved to accomplish the strategic cybersecurity goals.
R5	Governance	Stakeholder Awareness	Pointed to the decision makers through the whole chain of involvement for the cybersecurity strategy for projects, take into account that each individual has a different level of cybersecurity understanding. For an effective rollout and involvement of the different stakeholders to understand the importance of cybersecurity projects to the organization, use a method for actual and recurrence awareness as strategic importance. Normally decision makers do not have a cybersecurity as first sight into account when making a decision.
R6	Governance	Cybersecurity Business Risk	Put understandable cybersecurity projects and activities on the key performance dashboard and program of board and steering committees.
R7	Governance	Cybersecurity Business Risk	Have a clear understanding of risk, threat level and impact to the company in common but also risk appetite the company can handle or wants to expose themself
R8	Governance	Dashboard KPI	Define a strategic cybersecurity roadmap for the next 3-5 years
R9	Governance	Dashboard KPI	Build a yearly project program for cybersecurity with different priority categorization as KPI
R20	Value	Risk Framework	Make use of different frameworks, best-practices, active communities and take out what best applies to your specific environment and determine what is necessary to protect your business.
R21	Value	Risk Framework	Use threats, new developments as strategy for the strategic cybersecurity roadmap
R23	Value	Risk Framework	Good understanding of actual compliance and best practices. To stay up-to-date within this field is crucial using communities or public or paid services.
R24	Value	Risk Framework	Governance of implementing the company specific compliance and/or best practices by risk assessment of each subject translated to business risk and impact and capture with priority, right implementation sequence at the cybersecurity project roadmap or program.
R25	Value	Define KPI	Point the cybersecurity project and activities within the roadmap or program onto the related risk and impact
R26	Value	Risk Framework	Know if a counter measure fails to protect due to e.g. a vulnerability what the residual or new risk will be to the company.
R27	Value	Risk Framework	Selection of different best practices frameworks suitable to the organization,
R28	Value	Define KPI	Priority definition. How to define the right level of priority? Risk assessment and priority levels
R29	Value	Category	Categorization with Moscow principle for activities. What cybersecurity projects can have delay an how much delay permissible.
R30	Value	Define KPI	Business case for cybersecurity projects. Organizational value?
R31	Value	Category	Divide cybersecurity projects in different categories as business, upkeep and resilience
R22	Value	Define KPI	Put key performance indicators within the program and translate subjects into understandable language or risk for board level reporting.

Figure 25. Summarized requirements from interviews

Appendix C - Interview results

Governance: cybersecurity governance

The questions around cybersecurity governance were drawn up to introduce the interview, as well as to get a picture of how organizations deal with IoT and to gauge the cybersecurity maturity of the organizations. If cybersecurity is an important part, how is this carried out and sent using a top-down approach?

IoT future adoption or demand

Do you see a demand for IoT systems within your organization at this moment or in the future? Please explain, and if so, what is your opinion on the risk towards your organization? How will you mitigate these risk? Will this influence your current protection level? Will this demand also affect classified networks?

This question was asked as an introduction to determine whether IoT is a recent topic or important in the future, with the rationale that the current investigation showed that IoT has many vulnerabilities, and that adequate cybersecurity is essential. Several interviewees see the movements of IoT in the civilian market, such as wearables, self-ordering refrigerators, etc. The question is if this are real IoT systems. A direct application for the internal organization is still hard to imagine now. Still, although there are no concrete examples, some organizations are conducting actual research on this topic. Many organizations can see possibilities for the organization itself as a product. In fact, there is already demand for interconnectivity and certain applications within critical infrastructure. The dangers around IoT are also clear, agreement and protection around IoT must be an integral part.

Reflection with regard to the literature and questions

The literature investigation showed that a growth is expected regarding IoT. This expectation was also reflected in the interviews. It is difficult to visualize how this is and will be expressed within the corporate ICT networks. However, it is clear that there are major risks when using IoT. Several organizations are already busy with IoT developments and research for customers as a product. It is clear that IoT will be an important issue that needs to be handled with care. The right level of cybersecurity is crucial.

Requirement:

- Organizations have to be cyber resilient to adopt new technologies like IoT.

Cybersecurity budget benchmark

What is the percentage of the overall annual ICT budget for cybersecurity, and how is the budget spending divided between different cybersecurity categories (for example, technology, awareness, etc.)?

The interviews showed that the percentage of spending on cybersecurity is a tricky question. One is not aware of cybersecurity budgeting, however this will not directly indicate whether it differs from the average. It may be that this is a sensitive issue. A budget that is too large could signify that one is falling behind with investments or implementing measures, or it could also mean that cybersecurity is very important for the organization. A budget that is too small could mean that cybersecurity is not sufficient and that the necessary countermeasures may not be taken. A lower budget can also mean that certain cybersecurity activities are covered in other categories than cybersecurity budget.

It is striking that the more mature and large organizations have better visibility on their cybersecurity budget spending. This is more in line with the common benchmark. However most of the interviewees did not have a direct view on the cybersecurity expenditure, or did not answer this question. Only

assumptions can be made. A lack of budget may indicate the low cybersecurity maturity of the organization, or that budgeting of cybersecurity is divided into different budgets. A better indication may be specified in combination with the other questions.

Reflection with regard to the literature and questions

Several budget studies have been done, specifically on ICT cybersecurity budget spending. For example, the SANS institute, a cooperative research and education organization, indicates that the average payout for cybersecurity is 7-9%, and there is little difference in the size of the organizations. Small organizations spend around 6-7% on their cybersecurity budget, and medium and large organizations spend 7-9%. The main budget difference is in the organization type or sector; for example, the financial sector is above average at 10-12%.

The organizational cybersecurity budget can indicate how maturely the organization handles cybersecurity. Most of the studied cybersecurity budgets go to protection and prevention in addition to detection and response. A lower than average budget could mean that the organization has already implemented all controls, or that the level of cybersecurity receives less attention than it should. If that is true, then this is a potential organizational risk.

Requirement:

- A better overview is needed of spending at the cybersecurity at board level. KPI to benchmark own cybersecurity budget spending compared to any other similar industry organizations as a performance indicator.

Board involvement

How do you involve the board of directors in the importance of cybersecurity? What is the mutual expectation, and what are the best practices to get board-level attention?

It is striking from the interviews that there are only a few organizations that have clear cybersecurity alignment and control at the board level. Organizations do have reporting lines to the board of directors, but only for ad-hoc decisions and escalations. If there are urgent cybersecurity risk topics, these are turned to the board, e.g. in the case of an incident. There is more delegation of decision-making and more considerations around cybersecurity-related strategic priorities and projects. This is done at the level of responsibility of the CIO/ICT. Lowering the responsibility and control at the ICT level could result in a priority struggle. The CIO has the duty to deliver ICT services, support business innovation, and manage cybersecurity. Often with a shrinking budget, these delivery values compete with each other; this may result in an organizational cybersecurity risk. The whole decision-making process concerning running a business project or cybersecurity project depends on one person and his/her competence for understanding cybersecurity organizational risk. The more cybersecurity-mature organizations are clearly more mature in this competitive issue, by regularly involving the board of directors with the cybersecurity risk profile and progression of key activities.

Reflection with regard to the literature and questions

Information cybersecurity has evolved. Cybersecurity is an important part of business operations; it is not only the ICT department's concern, but a top-level responsibility (Gregg, 2010). Cyber risk can have a big impact on the business operations, but it is a complex topic. It is important for board members to know which cybersecurity projects contribute to the achievement of the business objectives and mitigate organizational risk. Board members must be aware of what risk the organization is exposed to and which project is key for mitigating that risk. The board should be able to manage risk and decision-making and not just react to incidents (KPMG Advisory, 2015). The NIST Cybersecurity Framework (NIST, 2014a) is a good example of coordinating cybersecurity activities at different organizational levels.

Requirement:

- There should be recurring board-level involvement and understanding of cybersecurity issues related to organizational impact.

Cybersecurity mandate

Does cybersecurity have a clear mandate at different levels within the organization? Are you able to overrule management priorities?

Within all interviewees' organizations, there is a clear mandate for cybersecurity. However, the mandate is often only used for escalations. It was indicated that the mandate must be used minimally to maintain one's credibility and effectiveness. In addition, within specific security-vital sectors, cybersecurity is concerned in all ICT decisions. When implementing a new project, the first step is to take cybersecurity into account within the project definition and requirement elaboration.

Reflection with regard to the literature and questions

A cybersecurity mandate serves "to give official permission for something to happen or mainly to order someone to do something." (Cambridge, 2016) A mandate is usually only used in cybersecurity if there is a need to make a decision because of high risk. This can for example be the cutting of the organization's Internet connection, or the implementation of a mitigation measure for vulnerability. Importantly, the mandate overrules other interests it is necessary, for instance in case of cybersecurity organizational risk. If an organization has issues the cybersecurity mandate, this also indirectly indicates how seriously it deals with cybersecurity.

Requirement:

- It is important to ensure that the mandate does not have to be required too far in advance. This can be done by clarifying ahead of time what the board-level expectations are around implementing cybersecurity projects that are carried out through the whole organization.

Steering committee

What kind of steering committees do you have for cybersecurity? What information does the steering committee or MT need to take adequate decisions regarding the priorities of cybersecurity implementations and projects?

It is striking that in less mature organizations there is no special steering group for cybersecurity. In contrast to small organizations and less mature organizations, there is consultation within ICT, and cybersecurity is often controlled with ICT budgets and projects. Decisions are taken on the basis of expertise, risk, and impact. It is a more informal process, with shorter lines and a strategic view to control projects. Board members are only involved when escalation is needed, instead of seeing organizational cyber risk management as a strategic value or program. A number of organizations have regular alignment with board member(s). The more mature organizations have a formal process in which business risks are translated into important projects, which are governed and controlled by the board. In the other organizations, steering committees fall mainly within the ICT department, instead of involving the business and/or the board of directors, and taking care of the risk as a strategic interest.

There is no single way with which organizations deal with cybersecurity projects in steering groups, or with which they decide which topics should be treated and which stakeholders or organizational layers must be involved in the steering of projects concerning cybersecurity risk.

Reflection with regard to the literature and questions

A steering committee has to point in the right direction. It is a dialogue between those who take a decision regarding the content and the management of a project. Steering or governing for enterprise cybersecurity means viewing adequate cybersecurity as a non-negotiable requirement of being in business. If an organization's management, including the board of directors, senior executives, and all managers, does not establish and reinforce the business need for effective enterprise cybersecurity, the organization's desired state of cybersecurity will not be articulated, achieved, or sustained. To achieve a sustainable capability, organizations must make enterprise cybersecurity the responsibility of leaders at a governance level, and not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance. Governance throughout the whole organization at the board level will set a direction, priorities, support change, and provide resources. It is critical that management ensure that adequate resources are allocated to support the overall enterprise information cybersecurity strategy.

Requirements:

- Senior management level. Set direction to ensure that resources are available to allow for prioritization of possible controls, and to allow countermeasures to be implemented on a timely basis and maintained effectively.

- KPI. Insist that management makes cybersecurity investments and cybersecurity improvements measurable, and monitors and reports on program effectiveness.

- Set up steering committees at the needed levels, including different stakeholders such as the board, business, and ICT. They need be involved to accomplish the strategic cybersecurity goals.

Cybersecurity awareness

What is the level of cybersecurity awareness and understanding among decision-makers relative to the importance of protecting the organization's interest or protecting it against threats? And are you able to overrule these decisions?

The interviews showed that cybersecurity is generally known within the organization because of public news or internal awareness campaigns. Specific sectors also have a vital function, and cybersecurity is one of the core values. The specific awareness level within the steering committee often depends on the individual. There are differences in culture, background, and personal interests. This is very important to know for cybersecurity decision-making, and continuous and specific personal attention is necessary. The less cybersecurity-mature organizations show that there is little visibility at the individual awareness level among the steering committee and board members. The more mature organizations are more specific about what is important in relation to cybersecurity awareness, such as individual qualities and knowledge level.

Reflection with regard to the literature and questions

For decision-makers of cybersecurity within the organization, it is important to know the importance of organizational cybersecurity to make educated decisions. Cybersecurity is often a complex matter and there are cybersecurity experts appointed within organizations to translate cybersecurity risk into business risk. However, the decision-makers have to know what the cybersecurity risk is for the organization specifically, understanding the organizational risk attitude and the consequences of postponing key cybersecurity projects, such as contractual compliance or laws and regulations. Failure to meet compliance can for instance mean that the organization will get a stop on delivery, penalty

clauses, or be rejected for new business assignments. It is therefore important to look not only at short-term decisions, but also at mid- and long-term goals or consequences.

Requirement:

- Regarding the decision-makers throughout the whole chain of involvement for the cybersecurity strategy projects, it is important to take into account that each individual has a different level of cybersecurity understanding. For an effective roll-out and involvement of the different stakeholders to understand the importance of cybersecurity projects for the organization, a method should be used to ensure actual and recurring awareness of strategic importance. Normally, decision-makers do not have cybersecurity as a concern when making a decision.

Value: cybersecurity risk and impact

Cybersecurity risk and impact are concepts with a broad context. A cybersecurity risk can manifest itself as a business risk, such as reputational damage, financial damage due to operational interruptions, loss of contracts or customers, retirement of the CEO, or even organization shutdown, such as in the DigiNotar case[2]. (NCSC, 2011) In the interviews with the experts, the goal was to bring forward cybersecurity causes or threats that can express themselves as risks, to indicate the importance of organizational cybersecurity resilience.

Risk/threat awareness

Are you familiar with the risk and threats that your organization is facing in the area of (cyber) cybersecurity? Please elaborate on how you stay updated and controlled within this field, for example critical updates, vulnerabilities, threat actors, etc.

The outcome of the interviews is that organizations focus on threat feeds, indicators or compromises, seminars, and news items. Organizations are resilient by staying up-to-date in the field of new threats. The more mature organizations are one step ahead with their number of different sources and their daily balancing of threats. What is striking is that a number of organizations do not use specific risk assessments, such as a business impact assessment or attack tree analysis, or an automated threat analysis, such as vulnerability scanning.

Reflection with regard to the literature and questions

To stay active with regard to new risk and threats, it is important to proactively stay up-to-date – especially considering IoT and the vulnerabilities that this development brings with it, and the published incidents related to it, such as the previously discussed Sony hacsansk. Proactive means giving constant attention to new possible risk and threats from and to the organization itself, for example with active vulnerability scanning and patch management, or by being subscribed to an early disclosure service of vulnerabilities and risk. These vulnerabilities and risks can indeed be exploited when not directly mitigated as they arise. The responses from the interviewees reflect the degree of maturity of the organizations dealing these risks. Reflecting that organizations use these inspections of risk and threats as input for term objectives, prioritization, and the cybersecurity roadmap.

Requirements:

- Make use of different frameworks, best practices, and active communities. Use what best applies to the specific environment and determine what is necessary to protect the business.

[2] In 2011 DigiNotar is hacked and fraudulent certificates are in circulation. This DigiNotar certificates are no longer accepted as safe.

- Use threats and new developments as a strategy for the cybersecurity roadmap. Put KPIs in the program and translate subjects into understandable language or risks for board-level reporting.

Compliance in practice

Are you able to comply with or implement all of the latest cybersecurity best practices, such as the SANS.ORG critical controls, within your organization? And are you able to comply with the latest regulated compliance requirements? If so, why are you implementing all controls? If not, why not, how come, and how much time is needed to do so? How do you know that the protection level is high enough?

Answering this question was difficult in practice because of confidentiality. The outcome of the interviews shows that not every organization is aware of available best practices within the cybersecurity domain. It seems that a number of organizations only use compliance requirements from, for example, contractual requirement agreements or general data protection regulation. A striking finding is that compliance requirements are especially easy to implement in business projects and existing environments, whereas it is much more difficult to implement new cybersecurity requirements or controls. Another striking finding is that not all best practices are implemented, but only what is necessary, and often on the basis of a risk assessment. Not every requirement is applicable. The more mature organizations also check the effectiveness of implemented best practices and compliance measures.

Reflection with regard to the literature and questions

Compliance in practice is meant to give organizations a clear view at the general organizational cybersecurity-maturity levels, and on how organizations deal with cybersecurity best practices and compliance requirements. Best practices are proven methods and solutions to protect business interests. This item is quite crucial to be cyber resilient and to be protected from general threats. Not all compliance requirements apply to an organization; these requirements should be considered based on a risk assessment by a cybersecurity expert. Being unaware of best practices and threats or not implementing the needed requirements for the organization will sooner or later result in organizational risk or in an incident.

Requirements:

- Good understanding of actual compliance and best practices. To stay up-to-date within this field is crucial using communities, or public or paid services.
- Governance of implementing the organization-specific compliance and/or best practices by conducting a risk assessment of each subject. Translating this into business risk and impact and assign priority. Using the right implementation sequence of the project roadmap or program.
- Putting understandable projects and activities on the KPI dashboard, as well as on the program of the board and steering committees.

Clear view on impact

If a cybersecurity incident impacts your organization's important assets, how would you describe the impact and damage to your business, your customers, and if applicable the societal impact? Can you elaborate on the possible damage figures?

The more mature and larger organizations do know the high level of impact to the business. They have a process in place to categorize the impact of an incident. The impact can be a fine due to regulation violation, or impact to customers or to the organization itself, even resulting in loss of business due to reputational damage. The impact depends on the incident type. Some of the interviewees found it

difficult to express the organization impact, or did not want to express it. The respondents from the less mature organizations did not have a clear view on the business or organizational impact.

Reflection with regard to the literature and questions

The impact of a cybersecurity incident can have destructive consequences for the organization. This is the main reason why an organization should invest in cybersecurity countermeasures. A clear view on the impact can help to prioritize cybersecurity projects at different organizational levels – strategic, tactical, and operational. The business or organizational impact is an understandable concern, even if you one does not know anything about cybersecurity. Impact can be financial, reputational, or even societal if the organization delivers services to societally vital organizations.

Requirements:

- Having a clear understanding of risk, threat level, and impact to the organization, but also of the risk appetite that the organization can handle or to which it wants to expose itself.
- Pointing the project and activities in the roadmap or program towards the related risk and impact.
- Knowing what the residual or new risk will be to the organization if a countermeasure fails due to a vulnerability.

View on important activities

What are the most important cybersecurity activities to protect your organization's important assets (technical cybersecurity improvements, patching, vulnerability scanning, awareness, etc.)?

The interview results do show similarities with regard to the important activities. In summary, there has to be a basic level of protection or cybersecurity hygiene to avoid the threats that an organization is facing, such as on the Internet. In addition, the activities have to be in line with the threats to important assets. The more mature organizations go further to a broader focus and understanding of the changing threat environment, and they have the agility to implement new technical cybersecurity improvements to get ahead of new trends. What stands out from the overall findings is that cybersecurity awareness is a really important activity because most of the problems occur between the keyboard and the chair! And it is not an easy task to professionals who sometimes think that they are aware of cybersecurity risk, when in reality they not experts in this field.

Reflection with regard to the literature and questions

Cybersecurity is a broad and complex subject. For a cybersecurity officer, it is important to know what to protect and how to protect it. The protection level is mostly based on the risk appetite and formal compliance level to which the organization should adhere. Several cybersecurity standards and frameworks concern not only technical protection, but also organizational processes and procedures. For example, a change process is an important process for cybersecurity. If the changes meet the cybersecurity requirements, then the change is well tested to go into production. Changes can have a huge impact on the organization if a new product is not well protected or vulnerable. In addition to changes, another important activity within the organization is the organization's cybersecurity awareness. An organization can be well technically protected, but an employee may still work around the organizational policy, for example by failing to send confidential documents to private emails or by using other applications than corporate ones for filesharing. This can bring risk to the organization.

Requirement:

- The selection of different best practices frameworks suitable to the organization.

New significant risk

How does your organization handle significant risk that has seemed to exist for many years, but that has so far not been exploited?

Most of the organizations do have an incident process in place, and if they face a new threat, there will be a risk and impact assessment with a proper response related to the organizational risk. No answer was given if there were doubtful situations, and a few interviewees did not answer this question.

Reflection with regard to the literature and questions

- Literature research examples of cybersecurity incidents as Sony and Target in chapter three shows that these organizations probably were not prepared against the facing cybersecurity threat. SANS (SANS, 2015)shows that the Sony hack probably could be prevented. To identify cybersecurity risk, best practice is to perform risk and gap analysis using best practices methods as described within chapter four. Using risk analysis the cybersecurity risk and the countermeasure cybersecurity project can be identified. Based on the organizational impact, the cybersecurity project priority should to be designated. The organizational processes for project and program management should implement the cybersecurity project timely. Important is, translating the cybersecurity risk into organizational priority and proper cybersecurity project management.

Requirement:

- Assess cybersecurity organizational risk. The organizational risk should be assessed using a risk management approach as ISO27005(ISO/IEC, 2011) or BIA(ISO/IEC, 2009).
- Use of best practices frameworks as described in chapter four.

Control: cybersecurity control priorities in practice

The goal of the expert interviewees was to learn how organizations set up their cybersecurity roadmap, how cybersecurity project priorities are determined, and how they deal with priorities that compete with the roadmap.

Cybersecurity roadmap and priority

Does your organization have a cybersecurity roadmap with different projects? How do you know what kinds of projects are needed, and how are the projects prioritized? How do you determine the start date, and is the original start date executed and implemented in a timely manner as planned? If not, what are the most common reasons and what would be the best approach to accomplish your cybersecurity roadmap?

A striking result is that a number of organizations do not have a direct roadmap. They know what is necessary, but it seems that they have short-term plans and not a strategic or tactical overview, but rather more operational needs. Projects are on the ICT budget roadmap, and if the priority is not high enough the project may be postponed to the following year. The priority of cybersecurity projects is handled in the same way as for ICT projects on ICT and business priority and the project business case. The more cybersecurity mature and larger organizations do have a roadmap, and this roadmap is adjusted within a special cybersecurity steering committee. In general, the project roadmap timing is based on business need, resource availability, and any priority of risk reduction.

Reflection with regard to the literature and questions

- The NIST cybersecurity Framework (NIST, 2014a) can be used as reference to establish a cybersecurity program/roadmap, or can be used to complement the existing organizational

program with cybersecurity projects. The NIST and other best practices in chapter four supports to analyze the needed cybersecurity projects for the program. To determine the start and due date depends on the organizational risk. The organizational risk should be assessed using a risk management approach as ISO27005 (ISO/IEC, 2011) or BIA (ISO/IEC, 2009, p. 42).

Requirements:

- Define a strategic cybersecurity roadmap for the next three-five years.
- Build a yearly project program for cybersecurity with different priority categorizations, such as KPI.

Priority definition

How do you determine the priority of cybersecurity project or activities (for example risk assessment regarding these cybersecurity threat areas)? If applicable, with whom do you align these priorities (for example, the steering committee) and how are they monitored, adjusted, or controlled? Can you describe the process?

This question aimed to give a clear view of the accomplishment of project priorities, and of the controls that ensure that projects are delivered in a timely manner, bearing in mind the Sony hack.

There are different outcomes to this question that can be used as requirement for the framework solution. To get priority, it is hard work to get the cybersecurity project on project agenda. One has to convince all necessary stakeholders to support the project based on its possible impact and benefit. Another interviewee discussed the projects on a monthly basis face-to-face with the responsible person. Other organizations do have as steering committee with involvement of business and ICT to determine project priorities next to ICT projects. In addition, external stakeholders such as supervisors are also involved in defining priorities and oversight. At another organization where cybersecurity is important, the cybersecurity officer will define what is mandatory in the roadmap.

Reflection with regard to the literature and questions

- The organizational risk should be assessed using a risk management approach as ISO27005 (ISO/IEC, 2011) or BIA (ISO/IEC, 2009, p. 42).
- According to the NIST cybersecurity framework (NIST, 2014a), a common flow of information and decisions should be at executive, business and operational levels. At executive level, the focus is on organizational risk, at business level the focus on ICT infrastructure risk management, and at operational level the focus on securing the ICT infrastructure.
- Monitoring and controlling cybersecurity projects should be done with best practice cybersecurity project portfolio and project management, a best practice is Prince-2 for managing projects successful (Fallis, 2013).

Requirements:

- Priority definition. How to determine the priority of cybersecurity projects
- Regularly align different levels within the organization.
- Monitor and control the project start and delivery date.
- Awareness of the stakeholders.

Project steering committee

Does your organization have a steering committee to follow and control cybersecurity implementations? Who is accountable and responsible? How do you control or prevent these project

from being delayed? Is there an escalation procedure to the board of directors, and if so how does this work?

The results of the IoT interview show that cybersecurity priority is one of the top issues within competitive ICT project environments. This question aimed to give a clear view of the project handling within organizations. Is it only managed within ICT department or does it involve different organizational stakeholders?

The results show that there are organizations where cybersecurity is a strategic organizational topic or value, the organization cybersecurity awareness is high, and cybersecurity projects are not discussed with competition. In other organizations, steering is mostly done within the ICT department, with sporadic escalation to the strategic level. In a few organizations, the more cybersecurity-mature and larger ones, there is alignment between the business steering committee, the board, external control, and oversight of stakeholder bodies. Most organizations do not have a recurrent process at different organizational levels, where for example the steering of cybersecurity projects is done with the involvement of the business, or decisions are made at the board level. They suffer from competing priorities between ICT projects and do have to work hard for attention and priority.

Reflection with regard to the literature and questions

- According to the NIST cybersecurity framework (NIST, 2014a), a common flow of information and decisions should be at executive, business and operational levels. At executive level, the focus is on organizational risk, at business level the focus on ICT infrastructure risk management, and at operational level focus on securing the ICT infrastructure.
- According to NCSC New Zealand, executives are responsible for managing and overseeing organizational cybersecurity risk management. Cybersecurity oversight activities include the regular evaluation of cyber security budgets, ICT acquisition plans, ICT outsourcing, cloud services, incident reports, risk assessment results, and top-level policies (NCSC-NZ, 2013).
- Monitoring and controlling cybersecurity projects should be done with best practice cybersecurity project portfolio and project management, a best practice is Prince-2 for managing projects successful (Fallis, 2013).
- The ISO/IEC 27001:2015(ISO/IEC, 2013b) and NIST SP 800-53(NIST, 2014b) include incident response and business continuity and recovery plans.

Requirements:

- Cybersecurity steering committees at different organizational levels, such as ICT, business, and the board.
- Right involvement of stakeholders and awareness.
- Project priority control instruments.

Recurring cybersecurity activities

How do you prioritize and control plannable cybersecurity activities, such as patching, cleaning firewall rules, audit admin accounts, etc. that are executed within your organization (e.g. agreements with responsible teams/supplier)? And are these activities done according to a previously discussed timeframe?

Next to implementing new countermeasures for cybersecurity, the operational cybersecurity maintenance of the current ICT environment is as, if not more, important. Attackers can make use of the failure to run the latest cybersecurity patch to infiltrate or compromise the organization or information.

All organizations have in common that they find cybersecurity patching very important. This is already business as usual, and organizations are prepared to implement critical patches if necessary, either immediately or on a monthly basis. Some organizations do not have a full IT department and use subcontractors who offer patching as a service, such as a Service Level Agreement (SLA).

Reflection with regard to the literature and questions

- Monitoring and controlling cybersecurity projects should be done with best practice cybersecurity project portfolio and project management. A best practice is Prince-2 for managing projects successful (Fallis, 2013).
- Prioritize projects using MoSCoW(Agilebusiness, 2008). Within a cybersecurity project where time has been fixed, understanding the relative importance of things is vital to making progress and keeping to deadlines. Prioritization can be applied to cybersecurity projects, requirements, tasks, products, use cases, user stories, acceptance criteria and tests. MoSCoW is a technique for helping to understand priorities

Requirements:

- Cybersecurity operational KPI dashboard for the steering committee.
- Controls for managing KPI.

Cybersecurity activity delays

Is the cybersecurity steering committee effective in treating all key cybersecurity activities with proper priority? If not, what kinds of activities (grouped)? And how do you secure these key activities on different organizational layers (operational, tactical, and strategic)? Please briefly describe the structure or process (for example patching, project cybersecurity requirements met before production, etc.).

This question aimed to obtain a clear view on the organizational gaps where cybersecurity does not have the priority that it should have. Unfortunately, it appears that this question could not be answered in this context. Few interviewees would not answered this question to privacy reasons.

Reflection with regard to the literature and questions

- According to the NIST cybersecurity framework (NIST, 2014a), a common flow of information and decisions should be at executive, business and operational levels. At executive level the focus is on organizational risk, at business level the focus on ICT infrastructure risk management and at operational level focus on securing the ICT infrastructure.
- Prioritize projects using MoSCoW(Agilebusiness, 2008). In an cybersecurity project where time has been fixed, understanding the relative importance of things is vital to making progress and keeping to deadlines. Prioritization can be applied to cybersecurity projects, requirements, tasks, products, use cases, user stories, acceptance criteria and tests. MoSCoW is a technique for helping to understand priorities

Requirements:

- Set-up steering committee on different organizational levels and different decision-making rules on those organizational levels.
- Categorization with MoSCoW principle for projects. What projects can have delay, and how much delay is permissible?

Competing priorities

According to a recent study, many organizations are struggling to implement cybersecurity projects and innovations because of different competing priorities within the ICT department. Do you have the same struggle? Please elaborate on your answer about the current state: what are the bottlenecks, and what do you think will be the best way to solve this problem?

For most interviewees, this was recognizable. Persuasion skills are necessary to convince different involved stakeholders. Others have cybersecurity as a strategic organization value and this is not an issue. A striking finding is that for new business demand, cybersecurity countermeasures are mostly not an issue, such as collaborating with the business for a new digital transformation plan or cloud adoption. For other activities within the day-to-day operational environment, this can be a problem. Then, a business case is important. The bottleneck mostly occurs with regard to decision-level awareness, technical cybersecurity knowledge, and available/shareable resources. Hiring external resources as a solution can be a problem, because of their lack of internal organization knowledge, and also because a new functionality must be adopted by the resource team members if they have to maintain the situation. Knowledge transfer is then also an issue. The more cybersecurity-mature and larger organizations involve or align with business and cybersecurity teams, and they teams are sized to handle cybersecurity needs as dedicated teams. These autonomous teams are the most effective.

Reflection with regard to the literature and questions

- According to the Internet of Things World (Security of Things World USA, 2016) survey most of the organizations struggle with competing priorities, resources and cybersecurity knowledge.
- The Silent Killers method for change (Beer & Eisenstat, 2008) is a best practice to successfully implement the change strategy for cybersecurity and awareness. Interest
- The Power vs. Interest Matrix (Mendelow, 1991a) supports the framework in being effective and successful within the steering committee or at the board level
- Sense making in order to achieve as broad a cybersecurity basis as possible using Weick's collaborative properties to adapt are the following (Korsten, 2003).

Requirements:

- Right balance of execution, dependency, resources, and priorities between programs and projects.
- Business case of cybersecurity projects.
- Defined projects in different categories such as business, upkeep, and resilience.
- Stakeholder cybersecurity awareness.
- Resource cybersecurity knowledge and availability.

Increased risk due to delay

Has the risk or threat ever increased because cybersecurity activities or projects were not implemented in time? What is the average increased period in time (week, months) and could this/did this impact the organization (for example, the Sony hack)?

This question should have given a clear view of the problem of increasing risk due to the delay of projects. However, this was a hard question that could not be answered, due to the sensitivity of the subject.

Reflection with regard to the literature and questions

- A case study called "Critical Controls that Sony Should Have Implemented" by SANS institute (SANS, 2015) confirms that the Sony cybersecurity incident could have been prevented by implementing specific countermeasures.

Steering project risk

Say you are ready to implement an important cybersecurity project and the budget is allocated, but you are not able to implement the project due to another project or lack of available manpower/resources. How do you, or how does your organization, handle this issue? What would be the best way to handle this situation?

Most of the interviewees referred to the standard escalation process for project escalation. The project's escalation decision is made based on the business risk and impact to business and other projects. If other projects are almost done, following projects can be postponed a couple of weeks. This process cannot be misused to delay more than three times. For one organization, this had never been an issue due to its cybersecurity core strategic business value. The escalation procedure is a good practice; however, the question is whether the decision is made at the right organizational level, or if it requires a more strategic involvement, or a board-level decision.

Reflection with regard to the literature and questions

- In the interviews it seems more like day-to-day short-term decisions. At a strategic level, the delay of a project can have a major impact on other activities or can expose the organization to unnecessary risk.
- If implementation of the cybersecurity project isn't possible because lack of available resources, the ICT department should have a back-up plan for high priority projects. A back-up as external resources which are already are familiar with the organization ICT environment.
- The implementation issue of postponing cybersecurity projects should be monitored and controlled with project tolerances as described in Prince-2 best practices(Fallis, 2013).

Requirement:

- Boundary controls of cybersecurity projects to align them with strategic organization objectives.

Appendix D - The four steps of successful governance change

Silent Killer for change

The Silent Killers method for change (Beer & Eisenstat, 2008) is a best practice to successfully implement the change strategy of the new decision support framework. What does it take to successfully implement a strategic plan? From an employee perspective, it requires leadership, teamwork, and strategic direction. Michael Beer and Russel A. Eisentat found this, and based on profiling organizations and a detailed analysis, they identified six "Silent Killers" of strategy implementation. These barriers must be avoided when implementing the new framework:

1. Directive top-down or a non-directive laissez-faire management style with a focus on administration rather then strategy.
2. An unclear strategy or conflicting priorities.
3. Lack of teamwork from the senior management team – instead, a focus on individual areas, protection of individual power, and little cooperation.
4. Lack of open communication and poor vertical communication – little listening on the part of senior management, and an unwillingness by those in units below to make suggestions to upper management.
5. Poor coordination across units or functions, organization silos.
6. Middle management not ready or without the skills to lead change

Individually, these six barriers are troubling. Together, they create a vicious circle from which it is difficult to escape. Beer and Eisenstat also provide alternatives for each of the killers. Organizations can become fast and agile only if the six Silent Killers are transformed into the six following core capabilities:

7. A leadership style that embraces the paradox of top-down direction and upward influence.
8. Clear strategy, clear priorities.
9. An effective top team, whose members process a general management orientation.
10. Open vertical communication.
11. Effective coordination.
12. Down-the-line leadership.

In summary, for successful implementation of strategies, leadership should set direction, delegate authority for specific projects, and hold implementation teams accountable (Beer & Eisenstat, 2008).

Power vs. Interest Matrix.

The Power vs. Interest Matrix (Mendelow, 1991a) supports the framework in being effective and successful within the steering committee or at the board level. Stakeholders or stakeholder groups are plotted in this matrix and the matrix can then be used to determine their potential influence. This matrix can be used to highlight possible threats from particular stakeholder groups when deploying a new strategy, or if there is a change within the organizational strategy, such as deploying a new decision support framework.

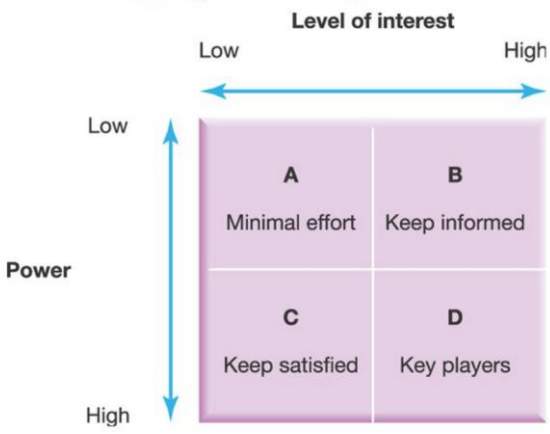

Figure 26. Stakeholder mapping: the Power vs. Interest Matrix (Mendelow, 1991b)

Mendelow's matrix (Figure 26) is a useful matrix for determining the potential influence of stakeholder groups on an organization. It looks at two dimensions: the level of interest that the group has in the organization, and the level of power or influence that it has over the organization. Power can be defined in many ways by the organization, from expertise in an area that fits with the organization's needs, to simply having a strong network of connections to which the organization requires access. The stakeholder group can take one of four positions in the matrix, based on its level of interest and power or influence (oxcomlearning.com, 2015).

- LOW POWER, LOW INTEREST: A stakeholder group in the top left is considered "minimal effort" and of little interest to the organization, as it is both low in interest and low in power/influence. This means that the group is more likely to go along with change with no resistance.
- LOW POWER, HIGH INTEREST: The organization should keep stakeholder groups in the top right informed. They have a high level of interest but do not have any power of note. However, due to their interest in the organization, they must be kept informed to prevent them from joining forces with other stakeholder groups and perhaps increasing their power.
- HIGH POWER, LOW INTEREST: "Keep satisfied" those in the lower left corner, with low interest in the organization but high power. Keeping these stakeholders satisfied will prevent them from gaining more interest and shifting into the "key player" box.
- HIGH POWER, HIGH INTEREST: These are the "key players" with both high power and high interest, and they are a very strong group that can oppose new strategy effectively and drive change if they so wish. It is up to the organization to invest in the relationship with these stakeholder groups by educating them as to the reasons for change to get them on board, communicating with them, and consulting with them to gain their support.

The cybersecurity organization can use the matrix to plot stakeholder groups regularly to highlight potential threats from these groups, or areas where a group may be able to assist. As a best practice, this is a particularly useful tool during times of strategic change, such as the introduction of a new strategy, or the modification of an existing one.

Cybersecurity wicked problems

The best practice below supports the cybersecurity change with the decision support framework to manage stakeholders within the complex cybersecurity environment, such as the (cyber) program steering committee.

Wicked problems (Camillus, 2008) are problems that are difficult or impossible to solve because of complex interdependencies. Solving one problem may create other problems. Wicked problems often

arise when organizations have to face constant change or unprecedented challenges. Cybersecurity and IoT are hard and complex to understand for different stakeholders. They change the organizational environment and processes, and call on the social context within the steering committee and disagreements between different stakeholders' own objectives. It is the social complexity of wicked problems as much as their technical difficulties that make them tough to manage. Rittel and Webber define ten characteristics to identify a wicked problem, and five ways to manage these wicked problems. The summarized five ways to manage them are the following:

- Involve stakeholders, document opinions, and communicate. The aim should be to create a shared understanding of the problem and to foster a joint commitment to possible ways of resolving it;
- Define the corporate identity; it must stay true to a sense of purpose;
- Focus on action that one is willing to take; and
- Adopt a "feed-forward" orientation; take unusual steps to move forward instead of the well-known roads.

Project portfolio

Portfolio management includes managing a group of projects and programs that bring together the new capabilities needed to one or more common business objectives. Portfolio management is the responsibility of the organizational management.

Portfolio management is there to realize the business objectives and to implement the necessary improvements on the one hand, and the available deployment of people and resources on the other hand. It involves a prioritization of the projects in relation to each other. The different projects sometimes jointly or separately deliver results or any added value for an organization. Portfolio management does not realize the added values in portfolio management, since this is done at lower levels of program management; it is only concerned with the delivery of the various projects in relation to each other (VHP, 2005, p. 169).

There are different portfolio methods that can be used within organizations to run the portfolio, such as the ICTPM or Prince-2. The best way to do this is to use the portfolio management method that is already used within the organization; to this end, other aforementioned approaches can be used.

When using the organizational or other portfolio management approaches, a number of considerations must be taken into account on the basis of best practices around risk. John Drake and Terry Anthony Byrd published a journal article about risk within IT project portfolio management. These risks will help to increase the success of cybersecurity portfolio management (Drake & Byrd, 2006). The cybersecurity project portfolio risk considers:

- ICT portfolio risk will increase when alignment between business strategy and ICT projects decreases;
- ICT portfolio risk will increase when core competencies are ignored in a project selection and prioritization;
- ICT portfolio risk will increase if the appropriate staffing resources are not available within the organization;
- ICT portfolio risk will increase when there is high ICT staff turnover;
- ICT portfolio risk will increase when there is high ICT management turnover;
- ICT portfolio risk will increase in an organizational culture adverse to change;
- ICT portfolio risk will increase when communication is hindered between ICT and business staff;
- ICT portfolio risk will increase when there are complex dependencies between projects;

- ICT portfolio risk will increase when there are complex project alternatives; and
- ICT portfolio risk will increase when financial measures of projects fail to capture the interrelationships between projects.

Appendix E - Sense Making

Sense making in order to achieve as broad a cybersecurity basis as possible using Weick's collaborative properties to adapt are the following (Korsten, 2003):

1. Identity and identification are central. Creating an identification context. As humans construct meaningful situations, they give themselves to who they want to be.
2. Retrospection provides the opportunity for sense making. Adjusting to the live experience of the context.
3. Sense making creates meaningful environments. Making the context meaningful. Sense making is not just about interpreting an environment that already exists, but about creating a meaningful environment. It is not only to look at, but also to evoke reality.
4. Sense making is a social activity. Creating social interaction about the context. The construction and interpretation of situations are created in the interaction between people.
5. Sense making is ongoing process. Creating frequent meetings about the context. Individuals simultaneously shape and react to the environments they face. As they project themselves onto an environment and observe the consequences, they learn about their identities and the accuracy of their accounts of the world. This is a feedback process, so even as individuals deduce their identity from the behavior of others towards them, they also try to influence this behavior.
6. People extract cues from the context to help them decide what information is relevant and what explanations are acceptable. Creating context where the stakeholders can create value for themselves, for example by letting the stakeholders tell about the Cybersecurity context. Extracted cues provide points of reference for linking ideas to broader networks of meaning and are "simple, familiar structures that are seeds from which people develop a larger sense of what may be occurring."
7. Sense making is more defined by plausibility than by accuracy. Creating a practical value for stakeholders' interest or business objective. People are focused on a useful and plausible picture of the situation, not on the exact analysis.