CYBER RISK GOVERNANCE

TOWARDS A FRAMEWORK FOR MANAGING CYBER RELATED RISKS FROM AN INTEGRATED IT GOVERNANCE PERSPECTIVE

Master thesis
28/08/2012 – Version 1.0

J.Geusebroek

Master Business Informatics
Institute of Information and Computing Science
Utrecht University

Universiteit Utrecht

Atos

Master Thesis

AUTHOR

Joost Geusebroek
Master Business Informatics
Institute of Information and Computing Science
Utrecht University

SUPERVISORS

Dr. R. S. Batenburg	Dr. M.R. Spruit	Dr. A. Shahim RE
Institute of Information and Computing Science Utrecht University	Institute of Information and Computing Science Utrecht University	Atos Consulting Nederland
First supervisor	*Second supervisor*	*External supervisor*
r.s.batenburg@uu.nl	m.r.spruit@uu.nl	abbas.shahim@atos.net

SUPPORTING ORGANIZATION

Atos Consulting Nederland

I. Preface

After finishing my bachelor degree the challenge of completing a scientific study at a university continued to draw. As I aspired to a career in IT, I decided to start the master Business informatics at Utrecht University. This master thesis is the final result of eight months research and entails the graduation project of the Master Business Informatics program. It has been carried out with support of Atos Consulting Nederland and Utrecht University.

During my study and this research, the world of science sparked me even more. Especially in regard of this particular research on cyber risk governance. I hope this research contributes to the scientific knowledge in this research domain and has its effects in practice, aiming at a more secure cyber domain in the future.

II. Acknowledgements

I would like to use this opportunity to thank and recognize the people who supported me during this research. Firstly I would like to thank my first supervisor Ronald Batenburg and external supervisor Abbas Shahim for their guidance, support and advice during this research project. Their expertise, comments, feedback and personal investments supported me trough the research process. I also would like to thank Marco Spruit for his contribution on reviewing this research as second supervisor at Utrecht University.

Secondly, I would like to thank the interviewees of Atos Consulting Nederland for the valuable expert input during this research. Especially I would like to thank Raymond Bierens, Roy Jansen and Rob Mellegers for their feedback, suggestions, enthusiasm and invested time.

Furthermore I would like to thank the people supporting me during my research for their patience, feedback and offering a helping hand when needed. Especially I would like to thank my girlfriend and parents for their unconditional support during my studies, despite the hardships they sometimes had to endure.

III. Abstract

Organizations become more dependent on IT (Information Technology) for managing critical business processes. The IT domain is a vastly changing and dynamic environment which evolves rapidly and is directly beneficial for organizations. However, this continuous changing environment implies new challenges for managing critical IT infrastructures in organizations, while maintaining the performance of primary processes, inter alia business continuity. One of the main challenges nowadays is to keep the environment safe from unwanted intruders assuring that the critical information of the company is kept safe and indoors. Unfortunately the chance of security breaches increase rapidly as a result of using more complex IT which contributes to vulnerabilities. In addition intruders flourish due to sufficient funding, input of low resources and tempting results which can be achieved. Organizations are on the verge of an increased number of attacks and are additionally more vulnerable to complex and sophisticated targeted attacks which both could harm critical business assets and affect their reputation.

It has become clear that organizations are not ready for the vastly ongoing changes of the IT environment. There is a lack of awareness regarding the potential risk facing and the negative outcomes which lie ahead. In addition investing in IT security does not contribute to financial benefits and is an attractive first target for budget cuts of organizations. The use of IT does not pose the initial problem per se; it is converging people, (business) processes and technology. Organizations show clear gaps on governing these elements structured and coherent. These organizations are reluctant to invest and to undertake and support these activities as well as lacking significantly in skills and knowledge throughout the organization.

This research focuses on protecting the cyber (IT; processes, information and technology) domain of organizations against cyber related risks, also defined as cyber risk governance (CRG). CRG refers to protection against cyber related risks and aims to mitigate unwanted consequences by coordinating activities between humans, processes and IT assets. Consequently this research supports organizations by supplying an executive instrument in order to protect against a continuous risk landscape.

The proposed instrument provides guidelines on how to cope with a changing cyber risk landscape. It entails an integrated governance perspective for managing cyber, people and processes throughout different levels of an organization. The instrument consists of two main models. The first model is a meta-model introducing four main components: risks, resources, response and reputation which form the basis for CRG. In addition the model visualizes dependency on external governance structures in addition to the own controllable CRG. Subsequently the meta-model is supported by a second model, a CRG framework which elaborates on these four main components by individual relation and operational characteristics of each component. Performing the instrument within the enterprise risk management processes will ensure a more clear and understandable organizational perspective on managing cyber related risks and supporting the coordination of cyber risk activities.

The hands on supportive managerial tool provides in addition to social scientific relevance via an elaborated scientific overview of the research field as this domain is still immature on scientific research.

IV. Table of contents

I. Preface 5
II. Acknowledgements 5
III. Abstract 6
IV. Table of contents 7
V. List of Figures 9
VI. List of Tables 10
1 Introduction 11
1.1 Research trigger 12
1.2 Research objective 13
1.3 Research questions 13
1.4 Research method 14
1.5 Scope 19
1.6 Relevance 19
1.7 Challenges 21
2 Literature review 22
2.1 Guidelines 22
2.2 Theoretical background 23
2.3 Security in cyberspace 24
2.4 Cyber Risks 26
2.5 Cyber Strategy 27
2.6 Related research 30
2.7 Conclusion 34
3 A practical view 36
3.1 Cases 36
3.2 Expert views on practice 41
3.3 Scenarios 42
3.4 Conclusion 44
4 Towards an executive instrument 46
4.1 Analysis 46
4.2 Framework analysis 48
4.3 Conclusions on analysis and frameworks 49
4.4 Instrument development 50
4.5 CRG meta-model 50
4.6 Continuous approach 53

4.7 CRG framework example cases 54
4.8 Validity 57
4.9 Retrospect 57
5 A first validation of the CRG framework 59
5.1 Outline interview 59
5.2 Content analysis – Interview Transcript Review 59
5.3 Semi structured expert interviews results 60
6 Conclusion 65
7 Discussion 69
7.1 Reflection 69
7.2 Validity 70
7.3 Limitations 70
8 Future research 72
References 73
Glossary 78
Appendix 79
Appendix A – Abbreviations 80
Appendix B – Overview cyber risk landscape 81
Appendix C – Expert validation interviews 82
Appendix D – Expert interviewees 106

V. List of Figures

Figure 1 – Integrated cyber governance view. Based upon model by Betz (2011). 12
Figure 2 – Research model 15
Figure 3 - PDD research project 17
Figure 4 - Positioning concepts based upon ISF (2011) 24
Figure 5 - Corporate governance view (von Solms & von Solms, 2006) 30
Figure 6 - Performance radial 42
Figure 7 - Consequences of cyber related risks based upon Ponemon Institute (2011) 44
Figure 8 - CRG Meta-model 50
Figure 9 - CRG framework 51
Figure 10 – Strategic cycle 53
Figure 11 - CRG framework in motion 54

VI. List of Tables

Table 1 - Research phases 14
Table 2 - Activity table 18
Table 3 - Concept table 19
Table 4 - Cyber threat overview 27
Table 5 - National cyber security strategies 29
Table 6 - Company overview 36
Table 7 - Cases overview 40
Table 8 - Expert interviewee's overview 41
Table 9 - External threat scenarios (Justitie, 2011) 43
Table 10 - Cyber risk governance framework description 52
Table 11 - Example case BYOD 56
Table 12 - Example case unknown targeted attack 57
Table 13 – Validation expert interviewees 59
Table 14 - Coding categories 60
Table 15 - Color codes transcripts 82
Table 16 - Expert interviewees first session 106
Table 17 - Expert interviewees second session (validation) 106

1 Introduction

Contemporary organizations face nowadays the dependency of using Information Technology (IT) systems for supporting their business processes. Upcoming technologies provide a rapidly evolving cyber landscape resulting in vastly outdating contemporary solutions. New technologies such as cloud computing provide organizations unprecedented scalable and financially attractive solutions. However, the lack of knowledge regarding these new and complex innovations poses potential problems for organizations. Storing sensitive information in "the cloud" for example implies transmitting information over the internet, making the physical boundaries disappear even more. Information is obscured in a web of technological innovation as well as the physical IT infrastructure. In addition stakeholders (e.g. employees, suppliers) are enabled to access the information whenever, wherever and however at their personal convenience. This is a great benefit for stakeholders; however it creates a borderless and complex digital environment which should concern organizations, inter alia regarding securing information in these systems. These new developments provide new threats such as theft of data, malicious attacks en possible new ways to commit organized crime (IT Governance Institute, 2007) with undesirable financial consequences. In the Netherlands the costs of cybercrime for the society are estimated at ten billion Euros per year, where three quarters of this loss is accounted for business and organizations (TNO, 2012).

Potential breaches and vulnerabilities in IT systems provide unwanted intruders access to the information without authorization. These intruders or hackers are characterized by their silent attack; they act anonymously, are invisibly present and usually detected when it is too late and the damage is done. The use of only a computer connected to the internet anywhere in the world, the anonymity and investment of solely time and knowledge provides an easy access platform for performing malicious activities. The usage of viruses, Denial of Service (DoS) attacks, vulnerabilities of IT systems and careless mistakes within organizations are examples of potential resources to support these kinds of activities. Hackers tend to be creative people exploiting these resources in congruence with logic and innovation striving to be one step beyond of organizations and software builders. To put it in a metaphor: hackers are nowadays not only focused on the box itself, but also on the treasure inside the box which is nowadays even more important.

Awareness is an important preliminary step to understand the potential threats of the IT risk landscape. However risk is not considered part of daily business. It is characterized as a burden, difficult and does not provide direct financial benefits. In contrary, it requires financial investments, time and people and is in addition an attractive first target for budget cuts of organizations. Next the interests of managers do not provide a prioritized focus on security of IT. Instead the focus if for example more on sales and other targets corresponding to their function requirements. This is often resulting in negligence with all its possible adverse consequences.

Securing IT systems and information processing is a pervasive concern of organizations. One benefit from a stable and trusted digital environment, eventually there is a major dependence on connectivity regarding these systems. Customer data, financial data and process data are examples of dependency on important information sources for supporting business activities, characterized nowadays as critical assets. In growing number of organizations information is the business (IT Governance Institute, 2006). Potential breaches in IT security could possibly result in misused

information which can harm organizations by affecting their financial assets, reputation and other damages. The loss of assets such as facilities, equipment and people are possible to be survived by organizations, however few can proceed with the loss of their customer data or critical information (IT Governance Institute, 2006). It is therefore of great importance to understand current threats, develop comprehensive knowledge and maintain a pointed strategy as well as an integrated organizational view to adequately identify and mitigate potential cyber related risks which can possibly harm the organization.

1.1 Research trigger

The cyber risk landscape evolved rapidly over the past decades. Possible security breaches provide unprecedented damages on vital assets of organizations. Figure 1, which is based upon a model by Betz (2011), provides an integrated view on the cyber governance landscape. The three pillars represent an overall tier view in the IT landscape. The processes pillar defines the logic layer which represents the way of thinking and reasoning of particular activities within the application. The technology pillar supports the application with the physical infrastructure of the system. In between the information pillar is situated, which represents the application itself and where the information is stored. Entering the information pillar through a malicious attack is also possible through the process pillar by defying the logic of the application or directly on the physical IT infrastructure itself with for example a DoS attack.

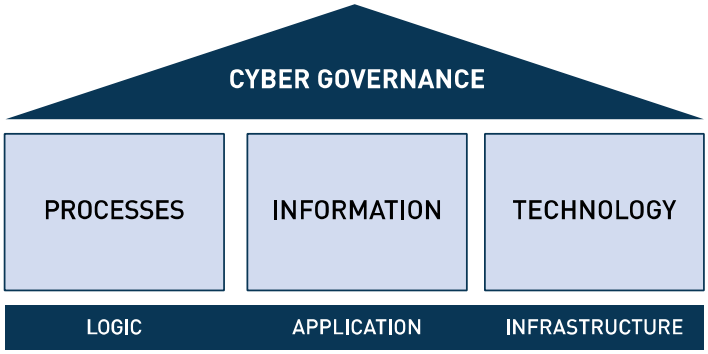


Figure 1 – Integrated cyber governance view. Based upon model by Betz (2011).

Much scientific research is conducted regarding each individual pillar. The technology pillar is for instance well supported by common standards and frameworks such as ISO 27001 and 27002 (International Organization for Standardization, 2012) or COBIT (ISACA, 2012) securing information through technology. For the information and processes pillar research is in abundance. Traditional research and approaches focuses on a bottom up approach by using technology as a starting point. However one should consider that IT risk is not solely a technical issue but also a business issue (B. von Solms & von Solms, 2004).

The cyber risk landscape is a tight congruence between humans and IT assets. Contemporary organizations face the difficulties of governing cyber related risks. It is an all-encompassing issue including leadership, accountability and adequate management skills. A top down approach considering a high level, domain independent and integral view on the cyber risk landscape from a governance perspective is relatively new and subject to research. Such an approach provides executives as well as managers a high level overview where technology eventually is a logical response for governing cyber related risks.

1.2 Research objective

The objective of this research is to contribute to the theory for managing cyber related risks from an integrated governance perspective by researching (scientific) literature, expert visions, executive cases and current frameworks methods and approaches. Comparing these frameworks and methods provide a comprehensive overview exposing possible gaps and flaws. The results of the research will contribute to the build of a new top down risk framework as a management instrument where people and processes are the foundation instead of solely technology. This ensures a balanced and resilient risk centric approach for governing cyber risk from an executive perspective.

1.3 Research questions

To support the research objective and achievement of the desired result the following research question is devised:

How can organizations manage cyber related risks in such a way that integrated governance is established in addition to securing IT infrastructures?

The main research question is based upon an integrated high level approach. No difference is made between organizations and their activities within individual domains (e.g. healthcare or finance). It consists of the three interconnected aspects; processes, information and technology depicted in Figure 1. In addition leadership and accountability is implied regarding managing cyber related risks. Finally the main research question proposed outcome is answered by a cyber risk framework which is intended as a comprehensible management instrument.

Based upon the main research question three sub-questions are derived which need to be answered individually to answer the main research question.

RQ 1: What are the current views in literature on establishing integrated governance for protecting IT assets?

Reviewing relevant literature prior to an academic project is an essential feature. Firstly an effective literature review provides a solid foundation for advancing knowledge. Secondly it facilitates theory development and exposes areas which are subject for extending the research field (Webster & Watson, 2002). In addition to scientific literature also grey literature is used for developing a theoretical background.

RQ 2: What do we see in practice with regard to cyber related risks influencing organizations in managing IT infrastructures?

The focus repositions from theory to practice. Many corporate cases can be found which provide lucrative information on cyber related risks, threats and vulnerabilities. By researching these cases different scenarios can be extracted which link certain actions or decisions to possible risks and threats. It provides an executive view in addition to the theoretical background.

RQ 3: How can an executive instrument be developed that contributes to integrally govern cyber related risks within organizations in order to secure information processes as well as IT infrastructures?

The answer to this question will be a conglomeration of the answers of the first two research questions. This in order to create a management instrument (framework) for organizations to govern cyber related risks within an organization and give a possible answer to the main research question.

1.4 Research method

The research is based upon the method of a design science research by Vaishnavi & Kuechler (2004). This type of research involves the design of novel or innovative artifacts to improve and understand the behavior of certain aspects in information systems. Vaishnavi & Kuechler (2004) present in their research the reasoning in the design cycle, which is based upon a study by Takeda, Veerkamp, & Yoshikawa (1990). This design cycle of research consists of five different stages. The awareness stage is to define the research trigger and the research approach. These are both elaborated in the introduction and research method chapters. The suggestion phase is to find possible answers to the research question based upon (scientific) literature found in this research field. In addition information is gained by interviews with experts from the field. The outcomes of the suggestion phase are used in the development phase attempting to analyze the results to build an instrument upon this information gained. The evaluation phase consists of analysis and expert interviews to validate the developed framework. The final phase is the discussion phase which describes the actual contribution of the research and is complemented with the conclusion section.

1.4.1 Research model

Figure 2 defines the research model of this study and is based on the method by Verschuren & Doorewaard (2007). The blocks represent the different research objectives within this research. The arrows indicate a conclusion of the research objectives resulting in a new merged objective. Next it defines the different relations of each objective and provides an overview of the structure of this research. In addition Table 1 (Takeda et al., 1990; Vaishnavi & Kuechler, 2004) is added to create a merged overview of the used research method in combination with the different activities and expected deliverables.

Phase	Step	Activities	Deliverables
I	Awareness	Research trigger and approach Desk research	Research trigger and method Theoretical background
II	Awareness and suggestion	Expert interviews Describe cases Describe scenario's	Research data (practical background)
III	Development	Analyze theoretical background in congruence with Phase II.	Concept framework
IV	Validation & Conclusion	Validation of instrument Expert validation	Executive instrument

Table 1 - Research phases

Phase I consists of performing a systematic literature review (Vom Brocke et al., 2009; Webster & Watson, 2002). Different sources are utilized such as scientific literature and grey literature. The literature study represents the current body of knowledge addition to cyber risk governance. The concepts chosen in the first phase represent high level key concepts of this research based upon the main research question. Each individual concept is researched complementing the background theory of this research. In addition current frameworks, methods and approaches which provide a high level overview based on previous defined concepts in phase I are added to this research. The first phase will constitute a solid work base for the next phase.

The second phase reflects the theory in practice. This is done by researching risk scenarios, actual security cases supplemented with expert input. The scenarios provide a comprehensive overview on potential risks by using IT solutions in particular circumstances; threats are directly linked to certain actions. IT security cases provide practical examples of organizations which encountered security flaws and breaches in their digital environment. This will provide information on the different kind of threats, vulnerabilities, actions and outcomes organizations face. In addition this phase is supplement with input from experts in the field in order to complement this phase with current proceedings in this area of research as well as providing input for the theoretical background (phase I) and this research in general.

Phase III is the analysis phase which coalesces the previous two phases into an extensive overview of all current findings. This phase represents the development phase in the design cycle research. Focus lies on the theoretical background in comparison with the other research objectives in this particular phase. The findings are compared and analyzed extracting the fundamental concepts providing solid input for development of the framework. Current frameworks, solutions and methods are studied revealing potential overlap and gaps. The analysis phase yields a concept version of the framework.

The final phase of this study is the development of the final framework as a partial answer to the research question. Primarily this phase is used for evaluation and validation of this research. The evaluation will be carried out by interviewing experts who will provide input on the framework based upon their experience and skills in the field.

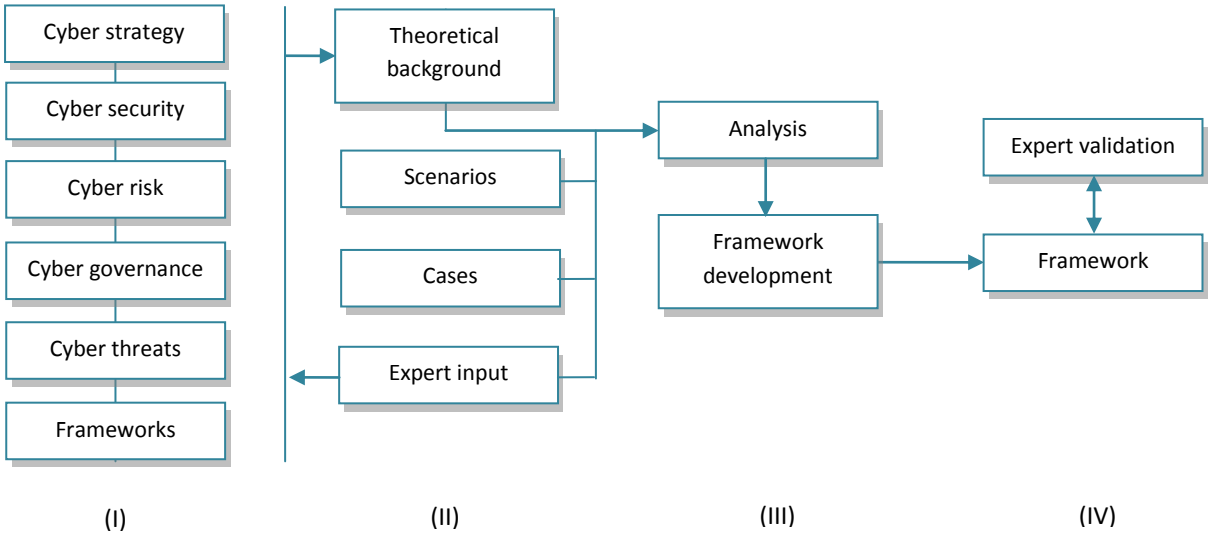


Figure 2 – Research model

1.4.2 Activities

To support the research method a Process Deliverable Diagram (PDD) is provided to describe the different activities and deliverables. The construction of a PDD is a practice based upon situational method engineering which is a useful approach for analyzing and constructing methods (van de Weerd & Brinkkemper, 2008). This diagram captures the entire strategy of this thesis project by defining the individual processes and expected deliverables of each activity. On the left the different activities are defined, on the right the deliverable of each activity is given.

In addition the activity table (Table 2) and concept table (Table 3) are provided to give a detailed description of each individual activity and to describe the different concepts of this research.

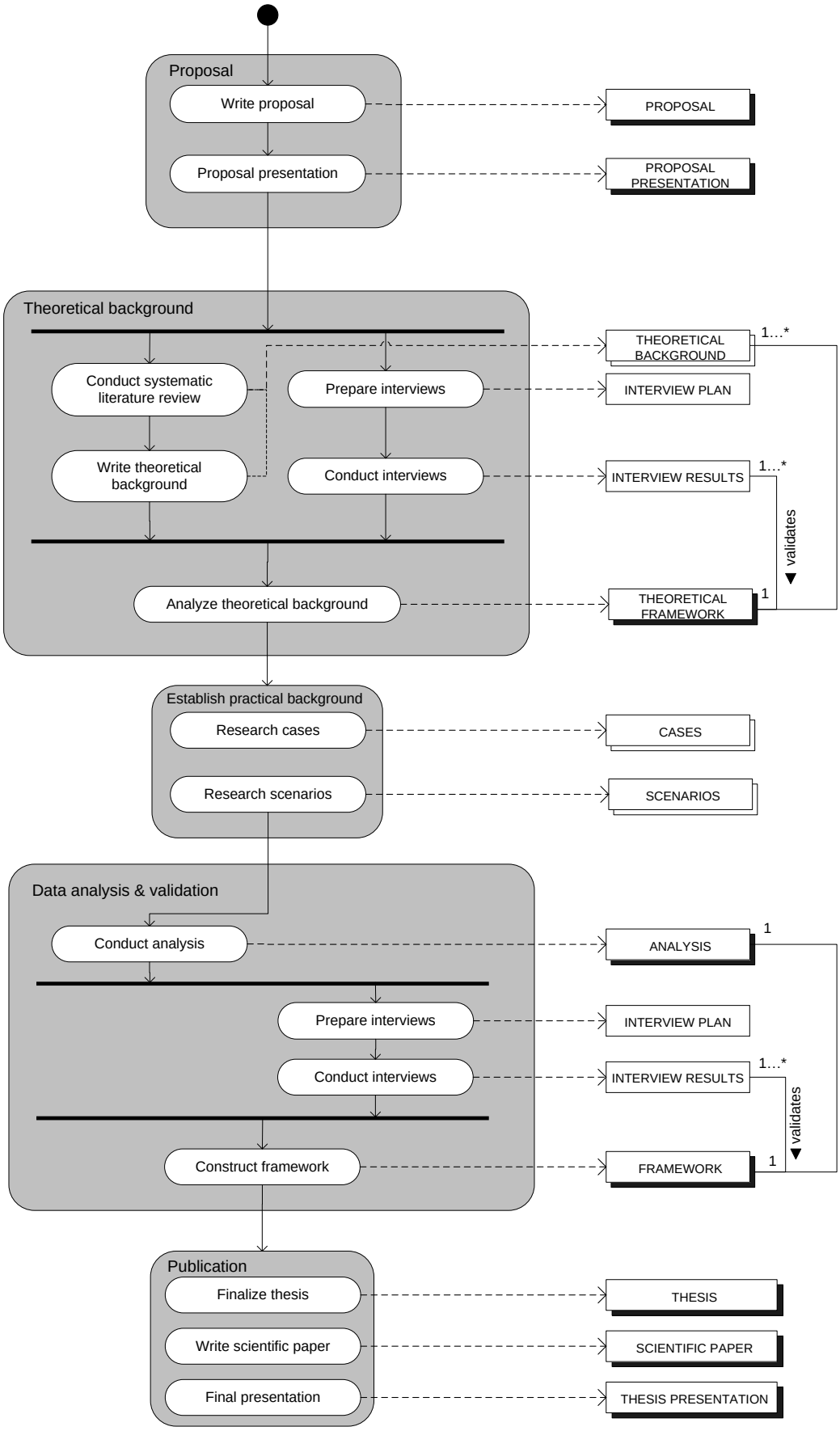


Figure 3 - PDD research project

Activity	Sub-activity	Description
Proposal	Write proposal	A proposal is the initial starting document prior to research. It consists of the global guidelines of the research.
	Proposal presentation	The PROPOSAL is introduced to fellow MBI students.
Theoretical background	Conduct SLR	The actual start of this research is conducting a Systematic Literature Review (SLR).
	Write theoretical background	Based on the SLR a theoretical background is constructed to create a body of knowledge.
	Prepare interviews	At the same time interviews with experts from the field are prepared.
	Conduct interviews	Interviews with experts from the field are conducted.
	Analyze theoretical background	All the information gained is analyzed and constructed to a theoretical framework. The concepts are positioned to each other and analyzed from different perspectives.
Establish practical background	Research cases	A shift from theory to practice. Practical cases are collected and analyzed.
	Research scenarios	CASES provide different scenarios which are analyzed.
Data analysis and validation	Conduct analysis	An overall ANALYSIS is conducted based upon all the information is gained. This will result in a concept framework.
	Prepare interviews	Interviews for validation of the concept framework are prepared.
	Conduct interviews	The interviews are conducted for validating the framework.
	Construct framework	The first version of the FRAMEWORK.
Publication	Finalize thesis	The merge of all parts of the research with the answers to the research questions will result in a THESIS.
	Write scientific paper	A SCIENTIFIC PAPER is written for publication.
	Final presentation	A FINAL PRESENTATION is given in order to complete graduation.

Table 2 - Activity table

Concept	Description
PROPOSAL	A proposal is an extensive document which is prior to research written. It consists of the global guidelines of the research, such as problem statement, trigger and research method. This results in a PROPOSAL.
PROPOSAL PRESENTATION	The PROPOSAL is pitched in a PROPOSAL PRESENTATION session introducing the research to fellow MBI graduates.
THEORETICAL BACKGROUND	A THEORATICAL BACKGROUND is created via a SLR (Vom Brocke et al., 2009; Webster & Watson, 2002)
INTERVIEW PLAN	An INTERVIEW PLAN is a preparation document for conducting an interview.
INTERVIEW RESULTS	The results of the interviews as a source for writing the THEORETICAL FRAMEWORK.
THEORETICAL FRAMEWORK	The complete analysis and positioning of the theory which puts it in perspective.
CASES	Recent practical executive CASES which provide 'real life' information.
SCENARIOS	The possible SCENARIOS which occur in correlation to certain cyber risks. These are extracted from the THEORETICAL BACKGROUND and the CASES.
ANALYSIS	ANALYSIS of all current research information in preparation of a concept FRAMEWORK.
INTERVIEW PLAN	An INTERVIEW PLAN is a preparation document for conducting an interview.
INTERVIEW RESULTS	The results of the interviews as a source for validation of the concept FRAMEWORK.
FRAMEWORK	The first version of the FRAMEWORK.
THESIS	The final document of this research containing all the research information and results.
SCIENTIFIC PAPER	A SCIENTIFIC PAPER is a small document describing the most important elements of this research to be publicized.
THESIS PRESENTATION	The final presentation of this research consisting of all the important steps and results of this research.

Table 3 - Concept table

1.5 Scope

This research will be conducted on an organizational view on IT related risks. As presented in Figure 1 the scope of this research is situated in the 'roof' of the model. The scope is maintained by not differentiating particular domains (e.g. finance or healthcare) or between different types of organizations (e.g. governmental or non-governmental). Finally an executive perspective is applied which puts managers and executives as a center point based upon their responsibilities, leadership and actions.

1.6 Relevance

This section discusses the relevance of this research distinguished on scientific and social perspective. The scientific relevance is examined by the empirical research elements in this study which contribute to the scientific research field. Secondly the social relevance is discussed based upon the value of this study regarding the society.

1.6.1 Scientific

From a general perspective this research contributes to the body of knowledge in the field of cyber risk governance. By providing a high level overview of this research area, a comprehensive overview is given from the current status of the research field. Due to current extensive research primarily focused on technical solutions a high level approach is a valuable addition to general research.

The individual deliverables of this research could possibly contribute to the research field. The literature study provides an overview of current empirical contributions consisting of theories methods and practices. Analyzing these contributions provide an extended and comprehensive overview of the conducted researches and how they relate to each other. Potential gaps and flaws are exposed which makes this study a valuable addition to the literature. In addition current findings from different practical cases will result in a clear view of contemporary problems which occur in organizations. Finally the framework provides a clear overview of the results in this study which contribute to the research domain by providing a hands-on instrument from a scientific relatively new point of view.

1.6.2 Social

Organizations nowadays face the increase vulnerability of using proprietary information in their IT environment. The digital environment is becoming increasingly more vulnerable to a widening array of risks that potentially can threaten the existence of an organization (IT Governance Institute, 2006). The range of threats such as information theft and malicious attacks make companies aware of the potential risks they are facing (Gordon, Loeb, & Sohail, 2003). Current research facilitates organizations numerous standards, solutions, methods and approaches to organize the security of their IT landscape. These are often bottom up approaches in relation to technology solutions. However a top down approach by giving managers the right instrument to provide control on their IT risk seems to be trivial.

This research provides organizations and managers a governance instrument for understanding the cyber risk landscape and how potential threats can be mitigated. It provides a high level overview and top down approach which organizations can use to assess their risks regarding their IT solutions. Assessing potential risks and threats in an early and pro active state provide organizations control mechanisms to mitigate the risk of potential harm and damage of crucial organizational assets. Next the framework contributes to making organizations more compliant to govern their IT solutions and conduces to the creation of awareness.

The final societal contribution is based upon the consumer. Consumer privacy is nowadays a common good which organizations benefit from. Possible security flaws do not solely affect organizations, but in many cases also the consumers. Stolen consumer information such as credit card information or a social security number is a potential source for committing identity theft by criminals. Securing the IT landscape is therefore not only of interest of organizations but also a societal issue. We all benefit from a safe and secured IT environment.

1.7 Challenges

Several challenges are faced during this research. The challenges appear in different phases of the research project and are described in chronological order conform this research. The first challenge regarding this research is finding suitable literature. Literature in the field of cyber security and risk is in abundance however scientific research from the proposed scope in this research is relatively new. Next to scientific literature also grey literature is accepted in this research. The control mechanisms on the quality of this literature are not comparative with the commercial scientific publishers. Literature needs to be well considered before applied in this research.

The second challenge is gathering information of cases from corporate organizations. Much information can be found in papers and news sections regarding practical cases. These sources could possibly consist of incorrect information, opinions from the authors, do not comply with the view of the organization concerned or vice versa. Special attention is needed to provide a complete and objective view on practical cases from different perspectives in this thesis project.

Next this research is dealing with a rapid evolvement of the cyber landscape in general. Cyberspace is a complicated, polymorphic and dynamic environment and evolving quickly (Geers, 2011). It is therefore a challenge to construct a research which is not short-term overtaken by the ravages of time.

Finally this research has several stakeholders such as compliance officers, risk officers and scientists. It is a challenge to combine both the vision of the executive stakeholders as well as academic stakeholders to meet both worlds.

2 Literature review

As researchers build upon previous developed research projects, research becomes a collaborative endeavor. Therefore a literature review plays an important role in new research projects (Vom Brocke et al., 2009). An effective review creates a firm foundation for advancing new knowledge (Webster & Watson, 2002).

The first part of this chapter discusses the guidelines for finding and analyzing literature to provide a comprehensive overview on the different steps made in this review. The latter part describes the breakdown of different concepts presented in phase I of the research model (Figure 3). These concepts will be discussed preserving a relation with cyber risk governance. Each concept is constructed based upon current definitions and underlying concepts found in the literature. These concepts are supporting in defining the taxonomy of the research field. The last concept (frameworks) will be explained by current frameworks which are related to this research and which can be used for inspiration.

2.1 Guidelines

The process of searching literature must be comprehensible described for re-using in future scientific research (Vom Brocke et al., 2009). The framework of Vom Brocke e.a. (2009) is used in addition to process the literature. It consists of five different steps for literature reviewing. These steps are described in the next paragraphs complemented with the steps and decisions taken for this particular literature review.

2.1.1 Definition of review scope

First and foremost step of the review is defining a clear scope. The proposed method of Vom Brocke e.a. (2009) is to draw on an established taxonomy for literature review by Cooper (1988). The author defined the following six characteristics: focus, goal, organizations, perspective, audience and coverage. Based upon these characteristics the review scope is defined.

The global focus of this review is on current theories. By looking into current theories and practices a common view is created to establish a common understanding of current (risk) problems and possible solutions. The goal is to find central issues which explain the underlying factors of risk. Organization wise the emphasis lies on finding methodological approaches to research the different steps needed. This will also contribute evaluate different methods. The literature perspective is based on a neutral representation. However, when necessary, the literature is positioned to other findings. There is no direct focus on a particular audience. It is hoped that the results will be of value for the general public, organizations as well as future researchers. The objective is to present a representative conglomerate view of current literature.

2.1.2 Conceptualization of topic

The second step is to create a broad understanding of what is known about the topic and which areas are subject for further research. It consists of a summarization of key issues which are relevant to the subject. This broad conceptualization is supported in the introductory part of this thesis project.

2.1.3 Literature search

Phase three consists of database, keyword, backward and forward search. It also includes ongoing evaluation of sources. Selecting journals, search databases and defining keywords allows for ensuring that the top-tier sources are included within the literature search.

Different database libraries are used for searching relevant literature. The searched databases are IEEE, Springerlink, Sciencedirect and ISI Web of Knowledge. These where selected based upon their relevance in the field of Information Science (IS). Google scholar is used for finding relevant literature which possibly is not available in the initial chosen database libraries.

Accepted literatures are books (including sections), conference proceedings, articles in academic journals and dissertations. In addition also grey literature is accepted; publications and whitepapers (inter alia grey literature) from relevant sources (established organizations or institutes).

2.1.4 Literature analysis and synthesis

After collecting sufficient literature on the topic the next step is to analyze and synthesize the literature. Collected literature is linked to the concepts which are presented in the first phase of the research model (Figure 2).

2.1.5 Research agenda

The synthesis of the literature is expected to result in a research agenda. It provides the base for further research in the field by pointing out white spots in current research and by posing sharper en insightful questions. The research agenda will be explained in the latter part of this chapter.

The next part will present the results of the literature review based on the previous described guidelines for conducting an extensive literature review.

2.2 Theoretical background

The concept ‘cyber’ has been used many times in the past decade to describe almost anything in relation with networks and computers (Ottis & Lorents, 2010). It is a common prefix for new terms such as cyber warfare, cyber attacks or cyber terrorism. The concept ‘cyber’ has an early history and originates from the term ‘cybernetics’ by Wiener (1948). Later on it transformed to the term ‘cyberspace’ which is nowadays more widely and common used.

In this research project the concept of cyber is an abbreviation for the term cyberspace. As there is still much debate on the exact description of this term (Information Security Forum, 2011) different definitions are mentioned and compared to each other. Ottis & Lorents (2010) define cyberspace as: “*Cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems”*. The authors added the time-dependency based upon the fact that changes in cyberspace can take place in an extremely short time span. Malicious code for example can spread out in minutes. Bodeau, Boyle, Fabius-Greene, & Graubart (2010) give a more detailed definition of cyberspace viz.; *“The collection of information and communications technology (ICT) infrastructures, applications, and devices on which the organization, enterprise, or mission depends, typically including the Internet, telecommunications networks, computer systems, personal devices,*

and (when networked with other ICT) embedded sensors, processors, and controllers". Which is in line with the definition by the Department of Homeland Security (2011): *"The interdependent network of information and communications technology infrastructures, including the Internet, telecommunications networks, computer systems and networks, and embedded processors and controllers in facilities and industries"*. The emphases in these definitions are more on the different types of technology leaving out the human interactive aspect of cyberspace. Ottis & Lorents (2010) argument that cyberspace is an artificial space, however without the presence of humans cyberspace would cease to exist. This factor is also present in the definition of cyberspace from the Information Security Forum (2011); *"Cyberspace is the always-on, technologically interconnected world; it consists of people, organizations, information and technology"*.

Technology is the premise in each of the definitions regarding cyberspace, however, it is not solely limited to it. Humans are a pivotal element in this environment. Cyberspace has unique characteristics which makes it a complex and constantly changing resulting in an unpredictable environment (Geers, 2011; Information Security Forum, 2011). Cyberspace is a defining feature of modern life. Between 2000 and 2010 global internet usage increase from 360 million to 2 billion people. Cyberspace will become increasingly woven into everyday life across the globe (Department of Defence, 2011).

2.3 Security in cyberspace

Different concepts regarding security are congregating in the domain of cyberspace, such as information security, cyber security and cyber resilience. Figure 4 provides an breakdown overview of the relation between the concepts information security, cyber security and cyber resilience positioned by the Information Security Forum (2011) based upon Confidentiality, Integrity and Availability (CIA) of systems. Threats in cyberspace are directly influencing these three concepts and are marked as the core concepts of information security.

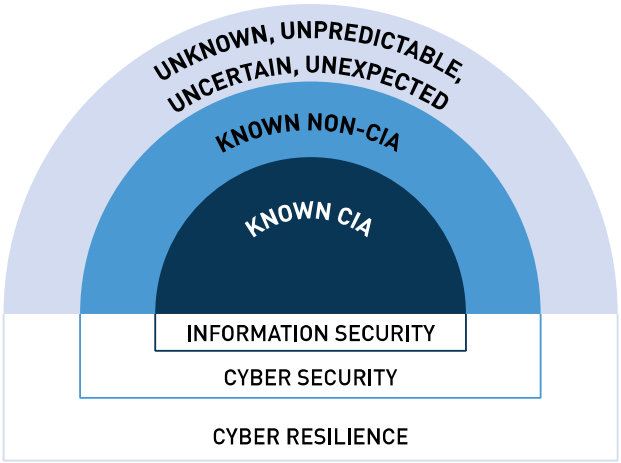


Figure 4 - Positioning concepts based upon ISF (2011)

With securing cyberspace one should address additional threats which are far beyond CIA, the known non-CIA. Examples are reputational damage due to a breakdown of the system or an unintended impact from leaking information. However, even cyber security is nowadays not sufficient enough. Organizations should understand that the rapid evolution of cyberspace is outpacing risk and opportunities. Security is no longer ensured to succeed. A current risk with a high impact which cannot be predicted, anticipated and mitigated is defined as the field of cyber resilience. The focus of this research is on cyber security; however, the other interconnected concepts are described as well in the next paragraphs to elaborate on the differences.

2.3.1 Information Security

As depicted in Figure 4 Information Security (IS) is based upon the concepts of confidentiality, integrity and availability and has a narrower focus in comparison with cyber security. These basic concepts can be found in different definitions of information security. Whitman & Mattord (2011) define IS as: *"To protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission"*. This is achieved via application of policy, education, training, technology and awareness. The definition of IS by ITGI (2006) is defined as follows: *"Information security addresses the protection of information, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organization"*. In addition the concept of IT security is often used and intertwined in combination with IS security. IT security is a subset of IS security as it s focal point is on the technology. Whereas IS security is not only focusing on technology but also on people and processes.

2.3.2 Cyber security

As mentioned in the introduction of this section cyberspace is a dynamic environment which provides many opportunities and significant risks. Securing the cyber environment is a main concern protecting organizations valuable assets in cyberspace. Axelrod (2006) defines cyber security as follows: "*The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems (and the information contained therein) to ensure confidentiality, integrity and availability*". This definition emphasizes the prevention and restoration of information and technology. The definition of the Information Security Forum (2011) is more broadened: *"Cyber security is the organization's ability to secure its people, information, systems and reputation in cyberspace"*. In comparison with the first definition the aspect of securing people is mentioned as well as its reputation in cyberspace. To access the organization and its operations people (groups or individuals) need to be authorized to access. Next the reputation is an important factor of organizations as it encompasses the confidentiality, integrity and availability. These concepts represent the trustworthiness of an organization. Organizational assets and reputation are the primary values at risk from cyber threats and vulnerabilities (The World Economic Forum, 2012). By the World Economic Forum (2012) cyber security refers to: *"Analysis, warning, information sharing, vulnerability reduction, risk mitigation and recovery efforts for networked information systems"*.

Cyber security is, in relation to information security, different due to an extended view on possible negative outcomes (e.g. reputation), which is not taken into consideration in information security. Cyber security focuses on additional threats which are beyond confidentiality, integrity and availability of systems. Cyberspace is an always-on environment. Organizations should understand the scope of this in correlation with potential threats and unwanted outcomes. Understanding and dealing with this environment is defined as the field of cyber security.

2.3.3 Cyber resilience

Cyber resilience stretches the scope of threats even more in comparison with cyber security. Cyber resilience covers an additional dimension of cyber risk management (The World Economic Forum, 2012). The ISF (2011) defines cyber resilience as follows: *"The organization's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace"*. Cyber resilience encompasses all the known CIA, the known

non-CIA and the unknown threats as depicted in Figure 4. Williams & Manheke (2010) defined cyber resilience in correlation towards small organizations as: *"The ability to defend against and to recover should a cyber incident occur and return to a normal functioning state"*. WEF (2012) shows a similar definition by stating: *"Cyber resilience is defined as the ability of systems and organizations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery"*. Cyber resilience differs from cyber security by taking into consideration that threats may occur and respond with a resilient approach to recover to a normal state. Taken into account a more broadened view on the likelihood of unknown threats is a different conception in relation to cyber security.

2.4 Cyber Risks

Cyberspace has many benefits for example innovation and collaboration. However in contrary to the many benefits, risks are everywhere. Risks are defined by Whitman & Mattord (2011) as the probability that something unwanted will happen. WEF (2012) defines cyber risks as: *"The probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation"*. In result cyber risks are a business issue with technical aspects which impacts all levels of an organization.

For organizations it is a continuously process of managing the risks versus the rewards (Information Security Forum, 2011). In this perspective organizations should manage their *risk appetite* or the quantity and nature of risk the organizations is willing to accept (Whitman & Mattord, 2011). However, most important is that an optimal models requires a program of understanding and mitigating risks with a risk management approach (Siegel, Sagalow, & Serritella, 2002).

2.4.1 Cyber threats

Threats in cyberspace can be found practically everywhere and are always present. Threats can originate, for instance, internally from personnel due to accidents or poor practice or external threats from unwanted intruders. In general a threat is a category of objects, persons, or other entities that presents a danger to an asset (Whitman & Mattord, 2011). A cyber threat is a potential cyber event that may cause unwanted outcomes resulting in harm to a system or organization (The World Economic Forum, 2012). Withman & Mattord (2011) make a distinction between purposeful and undirected threats. A purposeful threat is a preconceived goal such as extracting valuable information by a hacker from an organization. An undirected threat is for example a natural disaster threaten to affect physical IT infrastructures, such as fire. This distinction of threats can be extended by possible vulnerabilities of an organization. Due to poor practice, careless mistakes or by human failure or accidents possible cyber threats are more likely to succeed.

Not always is the physical infrastructure the main victim of cyber threats. Victims of cyber threats come in many forms and is not only limited to individuals, organizations and government. It also includes trust, innovation and collaboration or organizations (The World Economic Forum, 2012). Table 4 provides a global overview of possible cyber threats for organizations categorized based on Figure 1.

	Threat	Description
Processes	Software attacks	Attacks on the logical tier. For example Trojans, viruses, worms, DoS attacks to gain access or affect the information tier.
	Failure or errors	Usage of outdated software, bugs or code problems is providing holes in the system.
Information	Espionage	Unauthorized data collection and/or access compromising Intellectual Property.
	Human failure or errors	For instance mistakes or accidents made by employees regarding their information security responsibilities (e.g. managing their access credentials).
	Extortion of information	Blackmailing an organization to gather information.
Technology	Natural disasters	Natural threats which directly threaten the physical IT infrastructure (e.g. floods, fire, earthquakes or lightning).
	Failure or errors	Technical equipment errors shutting down operations such as disk failures.
	Force majeure	Dependency on third parties such as Internet Service Providers (ISP's) which possibly affects the availability of technology.

Table 4 - Cyber threat overview

There are many types of different threats. When focusing on purposeful threats WEF (2012) categorized four different types of cyber attacks. The first category is reconnaissance, gaining information from victims to plan a further attack. The second category is disruption for breakdown of business, system or service. Third category is extraction for extracting data from the victim. And the final category is manipulation for mutation of data or systems. CASI (2011) defines a cyber attack as: *"Generally an act that uses computer code to disrupt computer processing or steal data, often by exploiting a software or hardware vulnerability or a weakness in security practices. Results include disrupting the reliability of equipment, the integrity of data, and the confidentiality of communications"*.

A second categorization can be made regarding cyber attacks as Advanced Persistent Attack (APT) or Advanced Evasive Attacks (AET). APT owes their advance to a blended approach of computer intrusion (e.g. malware), social engineering (e.g. phishing) and the use of sophisticated management tools to analyze the attack. The victim can be anyone from government to business enterprises. An APT is not focused on a specific target, but persistent in attempts to gain access to it. An AET differs that it tries to evade or bypass security detecting during an attack (Georgia Tech Information Security Center, 2011; Winder, 2011). However, it is too early to state in this stage that these definitions will last.

2.5 Cyber Strategy

Governing IT is nowadays a daunting task in all layers of an organization. Organizations derive effective business processes with dependency on technology. IT assets support organizations in

achieving business goals. However, this technology drives complex governance and management challenges. In addition organizations are under pressure to enable trust and increase value for their stakeholders.

The growing use, adoption and dependency on (new) IT assets contribute to a fast evolving and complex environment which brings many challenges. The Cabinet Office (2011) defined the following challenges:

- The covert nature of threats brings possible underestimation of the risks facing;
- The prediction and understanding of cyberspace in the future is difficult due to the rate of new innovations and changes;
- New risks and vulnerabilities emerge suddenly;
- Responses and defenses look slow and inadequate due to the pace of events;
- Cyberspace is a complex environment; global in nature, largely commercially owned and consist of many different components, suppliers and sub contractors.

Nations, organizations and civilians rely on a secure and reliable cyberspace. Supporting the operational tasks of organizations and governments by creating a safe and secure cyberspace is a clear and well defined integrated strategy. The strategy should be part of an organization and integrated with Enterprise Risk Management (ERM) or larger security strategies within and beyond the enterprise (Bodeau et al., 2010).

Table 5 provides an overview of different national cyber strategies. These strategies show active nationwide strategies for a secure cyberspace. The individual strategies show different goals, as well as similarities which can be translated from governments to organizations, such as partnering and cooperation.

	Cyber security Strategy
Department of Defence (DoD) strategic initiatives (Department of Defence, 2011)	1. Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential 2. Employ new defense operating concepts to protect DoD networks and systems 3. Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy 4. Build robust relationships with U.S. allies and international partners to strengthen collective cyber security 5. Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation
UK cyber security initiatives (Cabinet Office, 2011)	1. Tackling cyber crime and making the UK one of the most secure places in the world to do business 2. Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace 3. Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies

	4. Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives
Dutch national cyber security strategy (GOVCERT, 2011)	1. Connect and strengthen new initiatives on cyber security 2. Cooperation between public and private sector 3. One (citizens, companies, governments) take their own responsibilities on cyber security 4. Every governmental department has its own responsibilities and tasks 5. Active international cooperation 6. Measures taken are proportional as there is no such thing as 100% security 7. Cyber security is reached at first on self regulation by companies and government. Legislation is involved when failing.

Table 5 - National cyber security strategies

Current existing strategies on enterprise level are mainly focused on information security, such as the COBIT framework. As cyber security is more than information security (see 2.2) achieving an enterprise-wide cyber risk strategy consists of different concepts which should be taken into consideration while defining the strategy. In addition a strategy is personal to every company. Organizations face different threats and have their own culture upon which the strategy should be constructed.

The department of Homeland Security (2011) used the following key elements of their own methodology for constructing a cyber security strategy for the homeland security enterprise:

- Assessment – of current and future strategic environment through analysis of key trends associated with cyberspace and cyber security;
- Examination – of current policy, strategy, programs and resources across cyber security activities;
- Identification – of key assumptions (including associated policy implications);
- Consideration – of alternative strategic concepts (achieve desired end states efficiently and effectively).

The following paragraph describes the cyber governance which explains the implementation of a strategy within the organization.

2.5.1 Cyber governance

As cyber risks affects all levels of an organization managing and prevention of these possible threats throughout the organization is self-explanatory. Management security activities should be governed continuously, consistently and correctly. Governance in general is a set of responsibilities and practices exercised by management (board and executive management) providing strategic direction. This in such a way that the set objectives are achieved, verifying that organizational resources are used responsible and that risks are managed properly (IT Governance Institute, 2006). In addition cyber governance refers to the component of enterprise governance that addresses the dependency on cyberspace in the presence of adversaries (Bodeau et al., 2010). Figure 5 (model based upon Direct-Control cycle by von Solms & von Solms, 2006) provides a corporate governance overview showing that all the layers (strategic, tactical and operational) of an organization are involved in

governing the strategic goals and directives. Cyber security governance requires and integrated approach and should be a transparent part of the corporate governance model of an organization. As cyber governance has a large focus on technical measures is seeks to influence human behavior and norms as well as processes and activities to prevent unwanted consequences (The World Economic Forum, 2012).

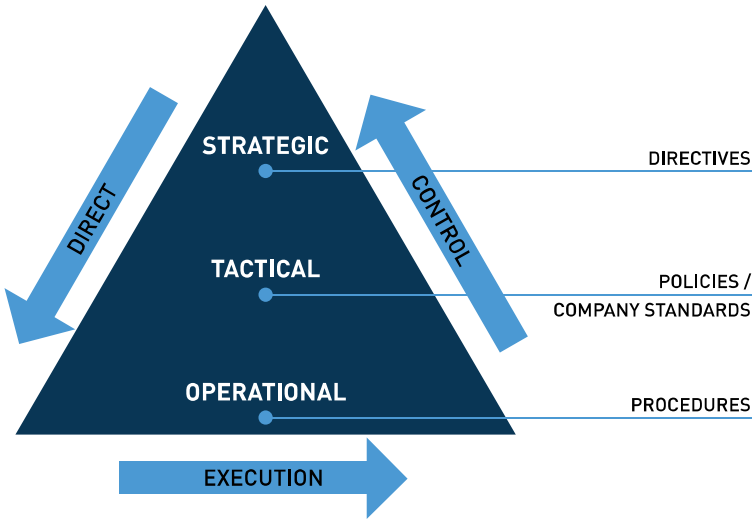


Figure 5 - Corporate governance view (von Solms & von Solms, 2006)

2.6 Related research

The final part of constructing the theoretical background is to analyze current research with regards to frameworks or instruments on governing cyber related risks. These frameworks provide an overview of the different steps and concepts the authors suggest for achieving a program of protecting organizations from cyber related risks. In addition to the previous described concepts it allows different views on how to assess and develop effective responses for possible threats and vulnerabilities. Furthermore analyses of these frameworks provide input for answering the first research question.

2.6.1 Frameworks

This paragraph provides a quick overview on the different frameworks which will be elaborated in the next paragraphs:

- *Cyber Prep framework (Bodeau et al., 2010)*
  This framework supports organizations by integrating cyber security strategies within an organization.
- *Cyber risk framework* (The World Economic Forum, 2012)
  A supportive framework for organizations to develop their own cyber strategy, it provides guidelines for organizations in order to create their own response.
- *The ISF Cyber Resilience Framework (Information Security Forum, 2011)*
  A framework which helps organizations to create their own (resilient) framework.
- *NIPP framework (Department of Homeland Security, 2009)*
  This framework consists of different steps for organizations to support organizations constructing an effective approach against cyber risk.

The latter paragraph of this chapter provides a summarized overview of the different frameworks. An extensive analysis is done in chapter 4.1.

2.6.1.1 Cyber Prep framework

Cyber Prep is a conceptual framework which helps organizations addressing adversarial threats related to its dependence in cyberspace (Bodeau et al., 2010). It enables organizations to defend against Advanced Persistent Threats (APT) by defining strategies. The framework consists of five levels of organizational preparedness:

- *Strategic integration*: to what extend is the cyber security strategy aligned with other organizational strategies.
- Disciplines: alignment of disciplines (or part of) regarding cyber security.
- *Risk mitigation approaches:* reflecting the priorities regarding compliance towards standards in correlation with investment in new mitigation techniques.
- *Adaptability / agility of cyber decision making:* the influence of adversaries on decision makers and decision processes.
- *Senior engagement:* determining the highest level of management which is engaged in cyber security decision making.
- *Cyber risk analytics:* identifying and assess risks which inform decisions.

These five levels relate to the organizations perspective on cyber threats, the strategy to address the threats and the approach to cyber security governance. Based on the organizations culture and risk framing the assessment of cyber security governance is conducted (in qualitative or quantitative terms, such as a score). The framework provides characteristics to assess the cyber security governance for each Cyber Prep level. The Cyber Prep levels are defined as follows:

- *Cyber Prep Level 1:* threats are largely externally and the organizations strategy is to defend the information system from malicious code/malware and discouraging unauthorized internal access. It uses commercial security software to defend the system.
- *Cyber Prep Level 2:* threats are largely externally. However, the organization recognizes that information is a target. Therefore safeguarding critical information (internally and externally) is seen as important.
- *Cyber Prep Level 3:* the organization understands that unwanted intruders are penetrating its information structure. Therefore a high degree of awareness is needed to identify and respond adequately to these threats. In addition procedures are constructed to better understand the adversary Tactics Techniques and Procedures (TTP's).
- *Cyber Prep Level 4:* the organization recognizes that it is not possible to keep the persistent threat from intruding the infrastructure, some may even be undetected. A strategy of architectural resilience is adopted to recover from a successful attack
- *Cyber Prep Level 5:* a continuous threat is assumed resulting in loss of key systems and services. Data has been purposely modified to mislead and confuse. The need for agility and flexibility is recognized. A highly agile and adaptive strategy is introduced to reshape (dynamically and continually) all aspects of the operating with regards to changing and successful attacks.

By assessing cyber security governance of an organization possible gaps or areas for improvement are identified. It supports organizations for making decisions about investment of security measures, aligning cyber security governance with other aspects of enterprise risk management and managing the awareness and attitude of the organization towards cyber security.

2.6.1.2 Cyber risk framework

The World Economic Forum (2012) created a set of guidelines for organizations to develop their own responses regarding cyber threats based upon the following principles:

- There is an increasing dependency for all organizations on connectivity. However resolving issues is a collaborative matter, not an individual matter. And even partners should collaborate to ensure a trusted and stable environment.
- The landscape of cyber evolves rapidly. Solutions are outdated rapidly and there are many 'unknown unknowns'.
- A continuous free flow of information drives economic values; a stand still will freeze the economy.
- One of the primary vulnerabilities of any organization is human awareness, leadership and execution.

The objective is to switch the mindset from solely securing the perimeters (creating a common mindset of shared principles) and include a focus on interdependency and resilience. Organizations accept that failures will occur and respond with a strategy of restoring normal operations ensuring the protection of assets and reputations. For common reference a maturity model is constructed consisting of five phases:

- *Stage 1 – Unaware:* cyber risk is seen as largely irrelevant and not part of the organizations risk strategy. The organization is also unaware of its level of interconnectedness.
- *Stage 2 – Fragmented:* there is a limited insight in cyber risk management and the organization recognizes their interconnectedness as potential risk. There is a funneled approach to cyber risk with incidental and fragmented reporting.
- *Stage 3 – Top Down:* the Chief Executive Officer (CEO) recognizes cyber risk management and initiated a top down approach for responding to cyber threats. However, this is not seen as a competitive advantage.
- *Stage 4 – Pervasive:* full ownership is taken with regards to cyber risk management. The organization is fully aware of the vulnerabilities, controls and interdependencies with third parties. It developed policies, frameworks, defined responsibilities and reporting instruments.
- *Stage 5 – Networked:* organizations are highly connected (peers and partners), sharing information and jointly mitigating cyber risk in their daily business. They are an industrial leader in managing cyber risk management. In addition people show exceptional cyber awareness.

To support the maturity model a high level cyber risk framework is provided based upon four main pillars; threats, vulnerabilities, values at risk and responses. Threats are divided in five different concepts (hacktivism (see chapter 3.1.6), corporate espionage, government driven, terrorism and criminal). The threats are correlated with the vulnerabilities (accidental or due to poor practice) of an organization based on people, processes and technology. In combination they put the organizations assets or reputation at risk. In addition to vulnerabilities, the final pillar is the responses pillar in order to mitigate the values at risk. The response of an organization can be traditional (policies or regulations), community (governance, information sharing, mutual aid and coordinated action) and systemic (risk markets and embedded security).

This framework provides organizations guidelines to prepare their own cyber risk strategy in mind that context will vary; organizations will create their own response. One main principle of this framework is collaboration among organizations in order to create a mutual effort for a stable and safe environment.

2.6.1.3 The ISF Cyber Resilience Framework

The ISF Cyber Resilience Framework (Information Security Forum, 2011) encompasses a broader view then cyber security. First it includes non-CIA threats to organizations in cyberspace. Secondly threats in cyberspace are magnified. The current impact on organizations regarding threats is from a different magnitude then a few years ago, which makes it difficult to compare. A final reason given is that adopting a broader view acknowledges the true scale of crime in cyberspace. This will create better understanding and response throughout the organization.

The purpose of the ISF Cyber Resilience Framework is to provide a reference model for an organization to create or refine its own cyber resilience framework. The framework consists of four main components:

- *A – Cyber governance and partnering:* the organization needs to have an effective cyber resilience framework for tracking cyber activities. In addition monitoring partner collaboration and risks in cyberspace.
- *B – Cyber situational awareness:* a process of gathering, analyzing and sharing of cyber intelligence should be incorporated in the organization.
- *C – Cyber resilience assessment:* a process needs to be available for assessing and adjusting resilience of the organization based on impacts from cyber activities in the past, present and future.
- *D – Cyber Response:* an effective response, prevention and detection process should be available to face cyber threats and minimize impact of potential threats.

The four main components define the global goals of the framework. Each component is attached to different related capabilities. The capabilities are defined in different criteria to assess the current position in the component.

2.6.1.4 NIPP framework

When focusing from organizations to a nationwide scale it is essential to ensure and protect Critical Infrastructure and Key Resources (CIKR). The Department of Homeland Security (2009) developed the National Infrastructure Protection Plan (NIPP) Risk Management Framework. This approach stretches from the cyber domain also to humans and physical assets. In this framework the cyber domain is taken into special consideration. This is due to the economic dependency on cyberspace, continuous attacks on cyber infrastructures and innovative technology, however, interconnected networks improves productivity and efficiency. Reducing cyber risk and enhancing cyber security is addressed in two ways, firstly by involvement of government and private sector owners and operators. Secondly in the responsibility of the IT sector in partnership with the communications sector.

The risk management framework consists of six steps which are overlapping three component elements of assets, systems and networks. These three components are represented as physical, cyber and human elements. The six steps are defined as follows:

- Set goals and objectives;
- Identify assets, systems and networks;
- Assess risks (consequences, vulnerabilities and threats);
- Prioritize;
- Implement programs;
- Measure effectiveness;

In addition there is a feedback loop from the last step across the other steps to the first step across the framework representing continuous improvements to enhance the protection.

2.7 Conclusion

The four presented frameworks show different views on how organizations can organize their cyber risk strategy in order to protect themselves from cyber related risks. Taken into consideration these differences the commonly found concepts in the frameworks are related to:

- Attitude – degree of situational awareness in an organization. Awareness supports the understanding of the necessity of an effective cyber approach.
- Assessment – defining which kind of cyber activities are needed as well as the current threat landscape of the organization (in terms of risks and vulnerabilities).
- Strategy – determining goals and objectives. Implementing the cyber risk strategy integrated in the organization such as conglomerating with Enterprise Risk Management (ERM) as well as involvement of (senior) management. Cyber security needs to be incorporated in all layers of an organization.
- Response – defining an effective (resilient) approach to threats and vulnerabilities.
- Partnering – partner collaboration (e.g. sharing knowledge) and networking.

The Cyber Prep framework and Cyber risk framework support the concept assessment in relation to a maturity model supporting organizations by assessing their current position in relation to a possible desired position. In chapter 4.2 (analysis section) the frameworks are addressed again in order to use them as inspiration for constructing an executive instrument in relation to this research.

Based upon the literature review, in combination with a preliminary view on the described frameworks, as well as focal points for consideration distilled from the collected literature, the first research question will be answered next.

RQ 1: What are the current views in literature on establishing integrated governance for protecting IT assets?

The cyber risk landscape is a complex, dynamic and unpredictable environment which evolves rapidly. In addition every organization is unique in its context, culture, business processes and IT assets which make it impossible to define one silver bullet solution to protect organizations from cyber related risks. Instead of searching for unilateral solutions one should define guidelines for organizations to govern their own cyber risk strategy.

Many guidelines or views are commonly used in the collected literature on establishing integrated governance. On organizational level a noticeable concept is organizational attitude and awareness. Organizations should be aware of a continuous threat landscape which is rapidly evolving posing major risks towards organizational assets and reputation. As there is nowadays no such thing as one hundred percent security, an organizational mindset is needed, focusing on these continuous risks complementing with an adequate response.

In order to create an adequate response an integrated approach is needed throughout the strategic, tactical and operational levels of an organization. As risk affects all levels of the organization integrated cyber risk governance should be conglomerated with the enterprise governance model. An effective integrated cyber risk approach is incorporated in the DNA of an organization. This should be supported by sufficient organizational resources such as knowledge, time and financial resources. In addition employees should have the skills and knowledge to govern their tasks in order to mitigate the risk of human mistakes.

Important in an integrated approach is the understanding that humans are the leading factor instead of the technology. Errors are often likely to be made by humans due to for example bad decisions or poor practice. Humans are an essential influential factor in protection organizational IT assets. In addition an approach is continuous and not based on interval. An effective approach consists of continuous assessment of cyber related risks, attack potential threats and vulnerabilities and mitigate outcomes of potential threats in order to protect IT assets. Possible threats affect the confidentiality, availability and integrity (CIA) of IT assets, which are taken from the information security perspective. In perspective of cyber security the negative impact is even higher taken in consideration the non-CIA, such as reputational damage.

Conclusively establishing an integrated governance approach for protecting IT assets is based upon multiple factors and dependencies. Main focus areas which attract the attention are awareness, understanding the complexity of the cyber landscape, maintaining a continuous approach and providing sufficient resources are the key elements for an integrated approach.

In addition this research proposes the following definition for cyber risk governance: *Cyber risk governance refers to protection against cyber related risks and aims to mitigate unwanted consequences by coordinating activities between humans, processes and IT assets.*

3 A practical view

The second part of this research consists of a practical view, expert input and researches different scenarios (see Figure 2). The collected information is used to extend the theoretical background from the previous chapter and will provide an answer to the second research question.

Unfortunately, the last decade provides many different cases of companies dealing with security breaches in their IT landscape. This chapter describes a selection of different cases which were recently widely reported in the news and subject in the public debate. These cases provide a practical view on what went wrong, their individual response for mitigation and recovery and how these organizations dealt with the consequences.

The second part of this chapter consists of expert input gained from interviews of experts in the field of IT risk. This information is gained by semi-structured interviews (DiCicco-Bloom & Crabtree, 2006). This type of interviewing allows emerging questions during the interview next to predetermined open-ended questions. It creates a conversation in conjunction with previous observed data for an in-depth interview obtaining qualitative research data.

The latter part of this chapter consists of creating scenarios from the previous obtained data, such as outsourcing security to IT specialists. These scenarios map routes of wanted and unwanted outcomes. It provides insight in the relation of different concepts and how they act in co-operation with each other.

3.1 Cases

For analyzing a practical view on the cyber risk landscape different recent cases (Table 6) which made the public press where chosen to analyze. These cases are chosen due to their high impact on society, targeted companies or organizations itself. Obviously these cases are the tip of the iceberg. The diversity of these cases provides insight in the attack and its consequences.

Company	Description
Diginotar	Dutch commercial CA (Certificate Authority), which was responsible for Dutch governmental certificates.
Stuxnet	Advanced worm targeted nuclear power plants in Iran.
Sony PSN	Online environment of Sony providing games and content.
KPN	Dutch telecom and IT services provider.
VCD - Humannet	Company providing Humannet, an application which stores information of employee absenteeism
Wikileaks / Anonymous	Example of hacktivism.

Table 6 - Company overview

The procedure for data collection is researching qualitative data of each individual case. This consists of information such as (news) articles, technical reports and possible views of experts. Each case is conducted to a qualitative content analysis (White & Marsh, 2006) for analyzing the gathered information. The objective is to capture the meanings and messages to extract understanding in purpose, why did it go wrong, what went wrong and what consequences subsequently emerged. To avoid triangulation as many different perspectives as possible are presented. Where necessary these

perspectives are reflected to literature. The cases are described individually and followed by an analysis and evaluation.

3.1.1 Diginotar

Diginotar is a security company which provided digital certificates for Dutch governmental websites. These PKIoverheid (Public Governmental Infrastructure) certificates served many online governmental sections, such as DigiD, the online identification method for Dutch civilians accessing online governmental applications.

In July 2011, during a daily routine check by Diginotar, 128 rogue certificates were detected, followed by several more later that month. A consequence of these rogue certificates was that web browsers indicate the website as safe and that the certificates were genuine, however in the same time these certificates could be used to derive information. Diginotar found evidence that these certificates where verified by internet addresses from Iran. This information was kept internal by Diginotar for about a month (Nightingale, 2011; van der Ploeg, 2011). On August 29th an SSL certificate was published online which apparently originates from Diginotar and presented to internet users in Iran ("Internet death sentence for DigiNotar's Root CA," 2011). A 21 year old Iranian hacker claimed the attack.

After this incident Dutch politics interfered by asking parliamentary questions about the safety and trustworthiness of governmental websites. In the following days Diginotar brought the news to the public of a possible hack, subsequently followed by the Minister of Home Affairs eliminating the trust in Diginotar as well as announcing measures ensuring trust in governmental websites (Wikipedia, 2012b).

On August 30th the company Fox IT was asked to investigate the hack at Diginotar (named 'Operation Black Tulip') and implement the necessary security measures. Fox IT (2011) came with the following conclusions:

- The successful hack implies that the current network setup and procedures at Diginotar were not sufficient to secure and prevent such attack;
- The password was not very strong and could easily be brute-forced;
- The software installed on the public web servers was outdated and not patched;
- No antivirus protection was present on the investigated servers.

As a result the servers contained malicious software which could be easily detected by antivirus software.

There were major consequences for the company Diginotar as well as all third parties related to the issued certificates. Web browsers did not trust the issued certificated by Diginotar anymore and were all revoked (van der Ploeg, 2011). This affects all third parties and service working with these certificates. After two months since the first detection of a possible hack Diginotar was declared bankrupt on September the 20th.

3.1.2 Stuxnet

In June 2010 a highly advance worm called Stuxnet was discovered by a Belarusian anti-virus firm at an Iranian nuclear facility. The Stuxnet worm was undetected and at least a year active on the internet (Falliere, Murchu, & Chien, 2011). Until then it was the most sophisticated piece of malware discovered yet (Geers, 2011). It consists of several zero day vulnerabilities (weaknesses in software unknown to the cyber defense community, which are used by hackers for malicious purposes), stolen certificates and is intelligent enough to activate in the correct environment. In this case it was a closed environment (not public through the internet) and transported via a USB stick (also called air gapped) to gain access (Farwell & Rohozinski, 2011).

Stuxnet targeted critical infrastructures, especially the systems to manage major industrial installations. These are systems referred as SCADA (Supervisory Control and Data Acquisition) in combination with PLC (Programmable Logic Controllers) to control devices, such as industrial fans. Infected computers used to program PLC's, affected the PLC to act randomly while giving correct feedback for positive monitoring the PLC. For example an industrial turbine could turn to overload while the process seems to be as usual. This could have some major consequences especially in a nuclear facility.

The Stuxnet worm is designed as a weapon; it penetrates into the environment and tries to take over control. Instead of conventional weapons to eliminated target, cyber space is used. It is a clear example of a possible cyber war which could emerge between different nations. There is also the possibility of involvement from other nations and even companies (Wikipedia, 2012a). Nations are nowadays capitalizing on technology whose development is driven by cyber crime which they are possibly outsourcing to non-attributable third parties including criminal organizations (Farwell & Rohozinski, 2011). In light of the Stuxnet outbreak more viruses were recently found and detected such as Duqu, Flame and Gauss. Complex and modular viruses which can be altered for different purposes ("Nieuw super spionagevirus Gauss ontdekt," 2012).

3.1.3 Sony PSN

The PlayStation Network (PSN) is an online environment from the company Sony providing multiplayer gaming and digital content. In April 2011 the PSN suffered from an external intrusion attack. Hackers penetrated the network and successfully retrieved personal information of the members in the network. As a result the personal details of approximately 77 million users were stolen and made the network unavailable for several weeks (according to Sony due to maintenance). The personal information consisted also of payment information and credit card numbers. The hack of PSN makes it one of the largest security breaches in history (Chung, 2011).

PSN was a potential target due to the amount of personal data stored in the network. It affected Sony not only for millions of dollars in damage, but also severe reputational damage. In addition governments inter alia United States demanded answers from Sony.

3.1.4 KPN

In February 2012 KPN, one of the largest Dutch telecom and IT service provider, was accused for leaking personal information of 500 customers. A list was published online including passwords for

gaining access to the mail environment of KPN. As a precautionary measure KNP disconnected the environment affecting 2 million members (Essers, 2012).

Many speculations followed including the use of obsolete systems to provide services of KPN. While KPN incrementally activated their services after the hack a new source of the leaked data was found. The personal information made public was retrieved from the database of an online web shop which consisted of 136.000 members, instead of the servers from KPN (Essers, 2012).

After the hack KPN made efforts to mitigate their reputational damage by apologize to their two million clients and providing refunds for the damaged caused. New investments are announced by creating an own 'war room' with experts and a CSO (Chief Security Officer) is appointed. In addition the clients are financially compensated for the outage of the system (Bakker, 2012).

Responsible for the hack was a 17 year old boy who was also responsible for other hacks including a hack at the Korean University (de Winter, 2012).

3.1.5 VCD - Humannet

In April 2012 a leak in the software of Humannet was discovered by Dutch television program Zembla (Zembla, 2012). Based on tips from a previous broadcast regarding the privacy of information from a third party using the application they received information about the security of Humannet from concerned IT experts. Humannet is an application which stores information of employee absenteeism. The database consists of up to 300.000 highly privacy-sensitive records containing medical records.

The software was not able to shield itself from SQL attacks resulting in a relatively easy access by a common security breach. It affected hundreds of companies associated with the software. This resulted in one of the largest personal and medical data leaks in Dutch history (ANP, 2012; Fox IT, 2012).

3.1.6 Hacktivism

Promoting ideological views with the use of cyberspace is defined as hacktivism (GOVCERT, 2010). This way of promoting provides an unprecedented power to spread a message. Recently an uprising regarding hacktivists was seen by groups such as Anonymous and LulzSec (Justitie, 2011). These groups were recently often in the news through unlawful attacks on information and systems. Anonymous is especially known as sympathizers from the Wikileaks affair by attacking payment companies which declined transferring funds to Wikileaks. LulzSec is more on high-profile hacks instead of bringing a political message, by making victims such as the NATO and Scotland Yard (Justitie, 2011).

Besides unlawful attacks through illegal activities, also lawful attacks are known. These are disseminated through different channels such as viral videos, blogs, boycotts, email campaigns and petitions (Information Security Forum, 2011). These attacks can cause severe reputational damage to businesses.

3.1.6.1 Wikileaks

Wikileaks is an international non-profit organizations founded in 2006 by Julian Assange. The organization publishes classified, private and secret information from sources that are anonymous (e.g. whistleblowers). Through their website millions of documents were published covering confidential information from governments and organizations such as documents about the war in Afghanistan Iraq and different documents from the Dutch Embassy (Wikileaks, 2012).

3.1.7 Case comparison and evaluation

Table 7 provides an overview of the described cases. The cases described differ from source, purpose and effects. This underlines once again the complexity of cyberspace. When an incident occurs it is not directly clear what the source is and what particular intentions are present (Justitie, 2012). Companies outsource in many cases their IT to third parties, which can be seen in the cases of Diginotar and VCD - Humannet. These sub-contractors provide services to organizations contributing to business disruption when an attack occurs. This also affects the individual responsibilities of these organizations; who is designated to take these responsibilities in case of an attack and which parties are, in the end, responsible for protecting sensitive and personal information?

Case	Type	Source	Result
Diginotar	Hack	Hacker	Revoked certificates affecting companies and organizations. Bankruptcy Diginotar
Stuxnet	Malware	Possible government or intelligence agency	Infected computers all over the world, especially Iran. Resulting in shutdown of nuclear power plant.
Sony PSN	Hack	Hacktivists (hackers group LulzSec)	Outage of system, reputational damage, financial damage
KPN	Hacker	Scriptkiddie/hacker	Downtime system, reputational damage, financial damage
VCD - Humannet	SQL injection	Journalism program	Downtime system for repairs, reputational damage
Wikileaks / Anonymous	Hacktivism	Whistleblowers	Downtime systems, reputational damage, confidential information made public

Table 7 - Cases overview

Threats occur from different sources, are always present and have their own individual goals. There is no trigger which should set organizations on guard and continuously assess their own cyber threat landscape. In addition the technology used is becoming more complex. This makes the likelihood of increasing the error sensitivity more plausible.

Next organizational awareness and attitude regarding possible risks was lacking in many cases. Basic mistakes were made on highly confidential information which resulted major consequences financial as well as reputational. Research amongst the cost and impact of cybercrime of American organizations (Ponemon Institute, 2011) states that, despite the widespread awareness of the impact of cyber crime, cyber attacks continue to occur frequently. This results in serious financial consequences for governmental institutions and businesses. With proper risk management procedures, governance and compliance the chance of these mistakes can be mitigated.

The IT environment is even more complex due to the collaboration between companies. Many organizations nowadays rely on third parties for managing their IT assets. In such a chain of collaboration it is hard to define the boundaries of responsibilities of each organization. In the case of VCD - Humannet hundreds of organizations are using this system which are (in)directly responsible for the information in the system. Systems are interrelated and connected increasing the complexity and vulnerability of IT assets. Organizations are possibly trusting too much on their third parties for securing their IT or they are significantly lacking adequate arrangements when relying on security of their outsourced IT.

3.2 Expert views on practice

This paragraph provides a summarized overview on different expert interviews (Table 8) which were conducted. Qualitative interviews were conducted as they expand the data collection process and more in-depth information is gathered (DiCicco-Bloom & Crabtree, 2006). The purpose of these interviews is twofold. Firstly it expands the theoretical background by providing feedback with a practical perspective. Secondly the interviews provide practical information which provides valuable input for answering the second research question.

	Position	Company
Expert 1	Cyber Competence Lead, IT & Risk Management	Atos
Expert 2	Security Principal, Technology Risk, IT & Risk Professionals	Atos
Expert 3	Head of Global PHT Defense and Security Portfolio Management	Atos

Table 8 - Expert interviewee's overview

The semi-structured interviews started by introducing this research followed by a reflection of the conducted expert interviews. Table 8 provides an overview of the expert interviews that were taken during this research project. The interviews are conglomerated as a single summarized overview preventing overlap in presenting retrieved information.

3.2.1 Expert summary

Cyberspace is indicated by the experts as a complex environment where incidents happen and threats are omnipresent. This view should be integrated and part of the organizational vision. By creating awareness and a common view of things that might happen possibly alleviates the lack of awareness.

This lack of awareness and interest can still be seen in many organizations. Possible indicators are due to a wrong attitude of organizations such as ignorance and lack of skills and knowledge. Cyber risks are not seen and integrated as a part of daily business. It is indicated as complex, takes a significant investment in time and does not provide direct financial benefits. Knowing the threats means that an organization should be in touch with the details posing problems in all layers of an organization.

The complexity of current IT systems contributes to the cyber risk landscape. Systems are interconnected to multiple parties which increases complexity. Organizations have their own policies, tasks and responsibilities which makes it complex to manage such individual ecosystem. It is in addition difficult to make major decisions, often these cannot be made by one single person in the

organizational structure. Organizations should work together based on shared responsibilities in order to understand and manage the IT infrastructure.

Indicated by the experts humans are a major source for vulnerabilities of an organization. In many security flaws humans are a major influential factor. The high workload of employees, lack of time, knowledge, skills are in contrast with the resources from the organization itself. Organizations should govern their resources, making financial decisions and providing sufficient time.

Many organizations support Bring Your Own Device (BYOD) making it possible for employees to use their own smart phone and tablet within the company. This brings additional threats and responsibilities. For instance, the employees should be aware of possible viruses and defend these by installing a virus scanner. For an organization it is difficult to manage security as they are not in direct control of these peripherals.

To manage the performance of an organization one expert presented a performance radial (Figure 6). It consists of four core principles for managing performance. Each individual core concept is connected to the three other principles mutually contributing to the overall performance. The model provides a high level overview of success indicators which indicates the performance.

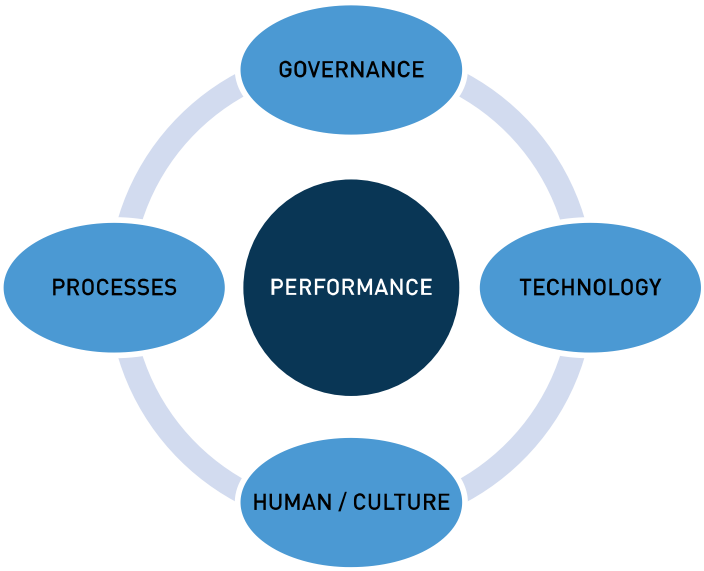


Figure 6 - Performance radial

3.3 Scenarios

The cyber risk landscape poses new complex problems that reach into new areas of national security and public policy (Lewis, 2002). This paragraph provides an overview of different scenarios which could occur by looking at the sources of the threats, external threats, internal threats and vulnerabilities of an organization.

3.3.1 External threat scenarios

As mentioned before threats in cyberspace are everywhere and differ from source to target. Nations, organizations and even civilians nowadays face the threats of cyber. Table 9 provides an overview of types of threats, sources and possible targets.

THREATS	TARGETS: Government	Private organizations	Civilians
States	Espionage/sabotage	Espionage/sabotage	
Private organizations		Espionage	
Hacktivists	Publication confidential information Digital disruption	Publication confidential information Digital disruption	Publication confidential personal information
Terrorists	Sabotage	Sabotage	
Criminals	Cybercrime Disruption of systems	Cybercrime Disruption of systems	Cybercrime (e.g. identity theft)
Scriptkiddies	Disruption of systems	Disruption of systems	

Table 9 - External threat scenarios (Justitie, 2011)

On nation-wide level the focus of threat scenarios lies on espionage and sabotage of systems in order to disrupt. Criminals feast on cybercrime activities for their own benefits. Especially civilians are possible victims in cases where personal information is stolen for committing identity theft or for instance the usage of credit card information purloining money. Scriptkiddies are as well a potential threat for government and organizations. These (often young) attackers with a lack of programming knowledge use developed programs and tools to infiltrate, disrupt and possible damage systems. Often the motive in these cases is wantonness and a pleasant thrill (Justitie, 2011).

3.3.2 Internal threat scenarios

In addition to external threats organizations face also internal threats. Employees acting from discord could possible damage information in systems as retaliation. The Stuxnet virus (see 3.1.2) was in all likelihood carried by an employee on a USB stick, infecting the systems as the nuclear plant itself is not connected to the internet. These potential threats pose possible major problems. Evidently organizations need to be aware of these types of threats.

3.3.3 Vulnerabilities of organizations

Vulnerabilities of organizations attract an increased possibility of cyber attacks, often attackers focus on these specific vulnerabilities to reach their goal. These vulnerabilities are due to possible mistakes or poor practice (Information Security Forum, 2011), where humans are protagonists of vulnerabilities. Technology could be obsolete, wrong or incomplete implemented. Business processes could not be complied incrementing frailties, or mistakes can be made due to possible ignorance; evidently in the end people do make mistakes.

3.3.4 Consequences

The described scenarios constitute to major consequences for an organization. Mentioned in this research are impacts on IT assets (confidentiality, integrity and availability), business assets (financial) and reputational damage. This provides a global overview on the impact of an organization when dealing with cyber related risks.

However, there are more consequences for an organization such as a possible aftermath of a security breach which still affects the business continuity, internally as well as externally. Figure 7 provides an overview of possible consequences which organizations face when dealing with cyber related risks.

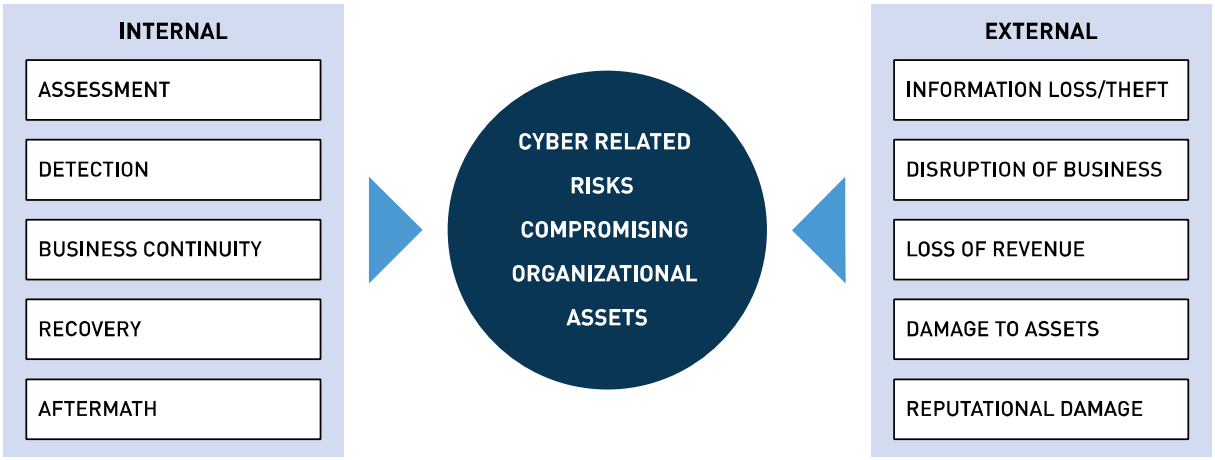


Figure 7 - Consequences of cyber related risks based upon Ponemon Institute (2011)

The predominant internal drivers affecting organizational resources are assessment and detection. When these drivers are compromised it affects directly business continuity with all its organizational consequences. Resources are needed for recovery and often there are aftermath actions needed to prevent future impacts.

Externally there is the possibility for information loss or theft and compromised confidential information which is made public, with possible damage in regards to IT assets. This creates a domino effect with possible disruption of business subsequently affecting revenue and reputation of an organization.

3.4 Conclusion

By analyzing different cases, interviews from experts on risk and presenting scenarios which occurs a more practical view is created. This part of the research is supportive in answering the second research question.

RQ 2: What do we see in practice with regards to cyber related risks influencing organizations in managing IT infrastructures?

The first part of the challenge is the complexity of IT nowadays. This makes it difficult to manage IT assets through all layers of an organization. Making the right (top down) decisions encompasses the right knowledge and sufficient resources which is lacking in many organizations. In conclusion two types of outcomes can be defined when IT is compromised due to threats: information theft and IT sabotage. Both outcomes pose major unwanted consequences for organizations such as influence on business continuity.

Next there is still an improper attitude amongst organizations by showing a lack of awareness and disregarding responsibilities protecting their digital business assets. Many organizations do not see governing cyber risk as part of their daily business. Individual interests (e.g. making more profit) are often more prioritized then dealing with cyber related risks.

Finally it is difficult to manage the individual responsibilities of organizations. Many organizations nowadays rely on the services of third parties. Systems are interconnected and managed by different sub-contractors. Defining each individual and shared responsibility in such a software ecosystem is a daunting task.

Organizations are facing difficult times experiencing more cyber attacks every year as well as an increased success factor of attacks (Ponemon Institute, 2011). Organizations need to be aware of the threats facing and change their behavior in order to face cyber related risk.

4 Towards an executive instrument

This first part of this chapter presents the analysis section (depicted in part three of the conceptual model, Figure 2) of this research. The analysis is based upon the literature study (chapter 2) and the practical view (chapter 3). In addition to support the development of the executive instrument, the different frameworks that are presented in chapter 2 are critically analyzed. Subsequently the construction of the executive instrument is described.

The analysis is done based upon the Qualitative Data Analysis (QDA) by Seidel (1998). The process of this method is based upon the following steps notice, collect, think and report. These steps are continuously used in constructing the analysis section as well as constructing the conceptual elements of the instrument. This chapter is in relation with the third and final research question which will be answered derived from the analysis section and the construction of an executive instrument.

4.1 Analysis

This analysis section strives for constructing an integrated cyber risk governance approach for protecting processes, information and technology while mitigating the influence of cyber related risks. Reaching this goal is done by seeking answers from the first two parts of this research, the literature review and the practical view on cyber risk.

Different concepts are collected (Seidel, 1998) which represents essential procedures for governing risks. Risks are seen as cyber related threats in combination with possible vulnerabilities of an organization. Protection is seen as managing risks; defer threats, minimize vulnerabilities and minimize the consequences (Department of Homeland Security, 2009) of possible information theft or IT sabotage. Subsequently the main end result is protecting organizational assets and reputation (confidentiality, integrity and availability).

Protection against cyber related risks is a continuous response approach throughout all layers of an organization. It encompasses a cyber risk governance approach which needs to be integrated in the enterprise risk management. Appendix B provides an overview of the initially found concepts which entail governing the cyber risk landscape. This conceptual overview is used to describe next paragraphs which contain the most important concepts for a continuous approach for organizational protection against risks and is used as a starting point for constructing the executive instrument.

4.1.1 Awareness

During the research on literature and interviewing experts the level of awareness was frequently returning and indicated as an important factor. Organizations need to be aware of the existence of cyber related risks in combination with the related consequences. In addition awareness creates the correct organizational attitude which is needed to prioritize protection IT assets and incorporate protection into regular business processes. As these tasks do not contribute to direct financial benefits or for example less work, it is important to realize the need of certain cyber risk activities. Next employees of an organization should embrace the same awareness and attitude to work attentively in order to prevent human errors and possible mistakes.

4.1.2 Assessment

In correlation with awareness assessment is of importance to assess the current cyber risk environment in relation to the organization and its current risk position. This position needs to be analyzed in relation with its current response to these particular risks. An effective assessment creates an as-is and to-be situation which clears the path for an associated response. This assessment also defines a clear maturity indication of the organization against the cyber risk landscape. The characteristic of assessment can be found on operational activities (in response to particular threats or vulnerabilities) as well as on a higher strategic level (supporting managerial directions) in the organization.

4.1.3 Response

The assessment phase clears the path for an effective response. This starts with detecting potential threats and vulnerabilities. Detection provides an outline of the risks that are faced, making a more effective approach possible. Awareness, assessment, detection and approach are the core concepts for defining a response against risks. Creating an adequate response for mitigating the undesirable outcomes is an essential process of recovery.

In addition two concepts can be defined which influence the affectivity of the response which are distilled from the different cases presented in this research. First responsibilities are introduced as the individual tasks need to be accountable to employees of an organization. These responsibilities could also relate to third parties which are present in the organizational cyber domain. Second additional concept which is introduced in the response component is partnering, often mentioned in literature and frequently encountered during the practical view of this research. Taking risks as a single organization is in certain cases more effective when partnering with other organizations. Sharing knowledge on events encountered could possibly contribute to a more effective (common) response.

4.1.4 Resources

An effective response is supported with sufficient resources. A distinction between IT resources and funding is made in this research. IT resources are supportive in providing the necessary elements for the construction and design of the cyber domain. Funding relates to the (organizational) resources for supporting an effective response. From an organizational perspective funding provides for example sufficient time for employees to conduct the necessary tasks, as well as financial impulses which are desirable for investing in corporate knowledge regarding cyber risks. Funding is also investing in the right people. Employees of an organization need the knowledge and the skills to cope with cyber risks. Organization should govern their resources in order to support effective approaches within the organization.

4.1.5 Govern complexity

Cyberspace is a complex and rapidly evolving environment. This needs to be maintained in an organization by continuously update (corporate) knowledge and skills. In addition making decisions top-down and bottom-up should be coherent and understandable. Involvement of senior management is of importance in a cyber risk strategy, however, the complexity of the concepts needs to be clear amongst all levels of an organization.

4.1.6 Manage continuity

Protecting an organization against cyber related risks is not a one time achievement. Protecting against risks is part of the regular business processes and needs to be incorporated in the DNA of the organization. Continuously assess the situation, detecting potential threats and vulnerabilities and maintaining an adequate and effective response is of key importance. All levels of an organization need to be aware of a continuous approach as well as incorporate cyber risk governance in Enterprise Risk Management (ERM) processes.

4.1.7 Strategy

Activities on operational level need to be supported by a strategy. Defining the strategy of cyber risk governance is encapsulating all the concepts for governing cyber risk. It entails as a first starting point for organizations defining overall objectives and directives. Derived from this research the strategy includes the concepts of assessment, approach and governance. Assessment is needed to define the current and desired position for establishing realistic objectives and directives against cyber related risks. It creates an as-is and to-be situation which constructs a clear direction. Subsequently the approach is defined which consists of high level agreements on how to achieve the objectives and directives in correlation with the results from the assessment step. In addition this step incorporates implementing the approach throughout the organization, embedding the approach in the Enterprise Risk Management (ERM). Final step is act, which entails the tasks and activities for achieving the determined strategy.

4.2 Framework analysis

Paragraph 2.6.1 provides an overview on current frameworks regarding cyber security. These frameworks are all in relation to this research and provide a supportive learning function. This paragraph analyses the frameworks critically and seeks for potential gaps or flaws in correlation with this research. As each framework fits its own purpose, there is chosen to look at corresponding concepts and differences. The best practices are used in order to support the construction of the executive instrument.

4.2.1 Cyber Prep framework (2.6.1.1)

This framework is used supports organizations to define and implement its strategy for addressing adversarial threats. It focuses on five levels which helps organizations to assess their current position and find a suitable strategy for protection against advanced persistent threats (APT). Predominantly this framework uses a business and governance focus to execute the strategy, which is effective for implementation purposes. However, the framework does not provide an integrated view on risk. For maintaining proactive protection against cyber related risk there is an integrated view needed on cyber itself in correlation with risk.

Explanations of potential risks are underexposed in this framework. The focus is on how to and why implement the strategy. It is not thoroughly explaining what types of risks are concerned. As the main goal of the framework is on implementation there is no focus on a continuous approach, which in correlation with this research is an essential element.

4.2.2 Cyber risk framework (2.6.1.2)

This framework provides a clear overview of the cyber risk landscape. In relation to this research it is underexposing the business focus. The framework is presented statically which underexpose the importance of a continuous strategy and approach in correlation with this research. Next it does not propose any activities to prevent potential threats and vulnerabilities; instead the framework focuses on the response.

In addition the described cyber landscape differs in comparison with this research. Technology, processes and people are described, whereas information is mentioned and people is not explicitly mentioned in this research. The integrated view on cyber (Figure 1) is based on processes, information and technology where people are incorporated in all three columns. Finally concepts as organizational awareness or resources are not mentioned in this framework.

4.2.3 The ISF Cyber Resilience Framework (2.6.1.3)

This framework is in conclusion a reference model to create or refine it to an own cyber resilience framework. The framework focuses on four main areas: partnering, awareness, assessment and responses. These concepts are frequently recurring in this research. The framework presents capabilities which can be used to measure and assess its position. The main focus is on business and is missing an integrated view on cyber (processes, information and technology).

4.2.4 NIPP framework (2.6.1.4)

This framework provides a quick and clear overview on cyber risk management and represents clearly a continuous (improvement) approach. The integrated view represents the layers physical, cyber and human which are present in all the given steps (see 2.6.1.4). The framework is missing a clear business focus: essential organizational elements such as awareness and resources are not mentioned. Next there is no focus on partnering or shared responsibilities in the framework, which is of essence in this research.

4.3 Conclusions on analysis and frameworks

The analyzed frameworks as well as the findings in the first paragraph of this chapter support in finding the main and essential concepts for the development of an executive cyber risk governance instrument. The concepts affect all layers of an organization: strategic, tactical and operational. As organizational differences make it difficult to map these concepts directly to these layers, a more broadened vision is taken to draw conclusions. Providing guidelines will enable organizations to map individual concepts to their own organizational structure.

Cyber risk governance starts with defining a clear strategy on the organizational approach. Defining the strategy that leads to policies which supports the operational (low-level organizational) activities. These policies are derived from four main concepts which are found in the analysis section: risks, resources, response and reputation. These four main concepts pivot continuously around the cyber domain of an organization to maintain a safe and secure cyber domain.

The next paragraphs will describe the development of a managerial instrument. Based upon the previous analysis section an executive instrument is constructed providing a clear and

comprehensible overview of the important concepts and their individual relations presented in the first paragraphs of this chapter.

4.4 Instrument development

The previous analysis section is the basis for the construction of an executive instrument for implementing and conducting cyber risk governance into an organization. This instrument is a constructed tool for managers in an organization to govern their cyber risks. The tool consists of a meta-model, includes a framework for structuring organizational activities and consists of exploratory content. The instrument is an auxiliary tool which provides guidelines for an organization. Therefore it can be mapped to the organizational structure and activities.

This paragraph describes the tool top-down by starting with the meta-model which provides a high level overview of the framework. Subsequently the framework is presented in combination with a strategic approach. In the latter part of this chapter, the tool is subjected on the basis of practical cases and includes a section on validity of the tool.

4.5 CRG meta-model

To support the cyber risk governance framework in simplicity and overview a meta-model (Figure 8) of the framework is created. This model consists of the main characteristics as presented in the previous analysis paragraph. The directives (strategy) encapsulate the four main concepts of risks, reputation, response and resources. These concepts are supported by policies and processes, to protect the cyber domain of the organization which is positioned in the center of the model.

Another characteristic depicted in the top of the meta-model is the possibility of multiple governance structures beyond the own organizational domain. When organizations outsource IT implies the adaption of (multiple) governance structures of third parties which are beyond control of the organization. Depending on (parts of) the governance of other organizations enables a collected governance structure amongst the chain of organizations. When this possibility occurs, organizations should conduct a dependency analysis making the dependency of other organizations and the influence on its own cyber domain clear.

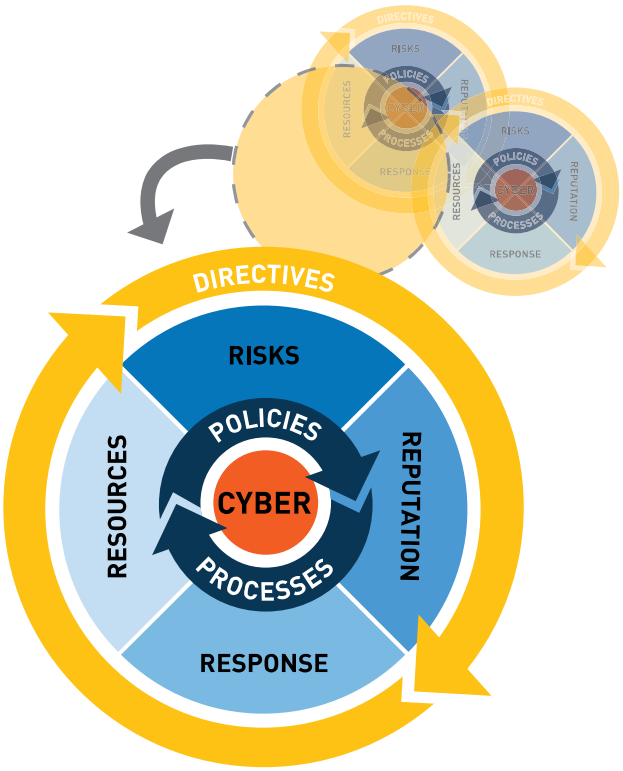


Figure 8 - CRG Meta-model

4.5.1 CRG Framework

The meta-model (Figure 8) is extended by the CRG framework. The four core concepts of risks, resources, response and reputation are elaborated by its characteristics and mutual dependencies. Figure 9 depicts the framework where the core concepts continuously pivot around cyber which is centrally positioned in a continuous approach. Each of these concepts needs to be supported with policies and processes from the organization.

The main concepts influence or determine the position of cyber. Risk and response are positioned on the opposite side of each other. Risks are directly of influence on cyber as well as the response preventing and mitigating possible unwanted consequences of risks. A secured cyber domain and an effective response against cyber related risk is depending on sufficient funding and resources. The response and the establishment of the cyber domain determine in their turn the strength to withstand the possibility of information theft and IT sabotage. This defines the safety of the reputation of the company ensuring organizational reputation and assets.

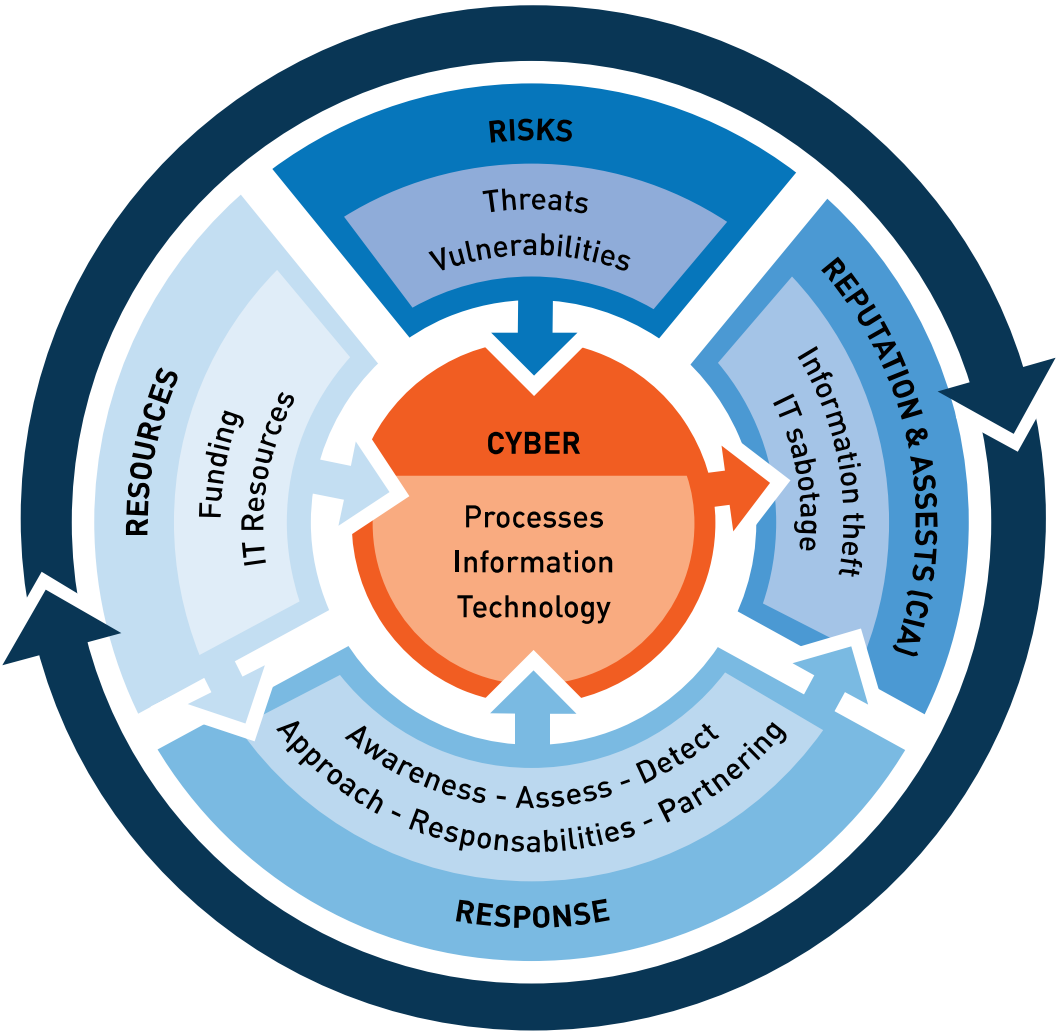


Figure 9 - CRG framework

Table 10 is provided to present an overview of all the individual characteristics related to the core concepts of the framework.

Main concepts	Sub concepts	Description
Cyber	Processes	Represents the logic layer of cyber. Bypassing the logic layer possibly leads to Information theft.
	Information	Represents the application layer of cyber and stores the information.
	Technology	Represents the technical infrastructure of IT assets. IT sabotage affects this layer affecting the confidentiality, integrity and availability of IT assets.
Risks	Threats	Possible threats emerging from the cyber risk landscape which threaten business reputation and assets.
	Vulnerabilities	Possible vulnerabilities of an organization reinforcing and nurturing threat potential.
Resources	IT Resources	Technical resources for maintaining and constructing a safe and secure cyber domain.
	Funding	Employees have the right skills and adequate knowledge preventing accidents or possible wrong performance. The employees are supported by organizational resources to receive time and space for doing their operational tasks. The organization invests in their cyber risk governance program. Constructing organizational awareness, knowledge and supply sufficient resources (time/financial) for conducting the necessary tasks.
Response	Awareness	The organization is aware of the potential risk it is facing in correlation with possible unwanted consequences.
	Assess	Assessment of the cyber risk governance strategy is continuously executed ensuring adequate position of the organization for risk protection.
	Detect	Risks are adequately detected followed by an effective approach for eliminating risks.
	Approach	Organizational approach for mitigation and minimizing the consequences of a direct threat.
	Responsibilities	Cyber risk governance strategy tasks are delegated to the employees which makes them responsible for their designated tasks.
	Partnering	Sharing information with partners to jointly mitigate the risk of cyber related threats. Next organizations have made agreements and insight in the individual and shared responsibilities for governing the (shared) IT assets.
Reputation & assets	Information theft IT Sabotage	The organization provides an adequate response to mitigate the consequences of possible information theft and IT sabotage. In addition it ensures the confidential, integrity and availability of the IT assets and conduct activities to preserve non-IT related consequence such as the reputation of the organization.

Table 10 - Cyber risk governance framework description

4.5.2 Strategy domain

The CRG framework (Figure 9) is supported and encapsulated with a strategic context also depicted in the meta-model as directives (Figure 8). Defining a strategy on cyber risk governance consists of four interrelated components (Figure 10). The first concept is to create realistic strategic objectives and directives. Realistic in a sense that security breaches may occur due to internal and external threats so that the organization is prepared to undertake the necessary steps. The organization also understands the necessity of security in its regular business processes.

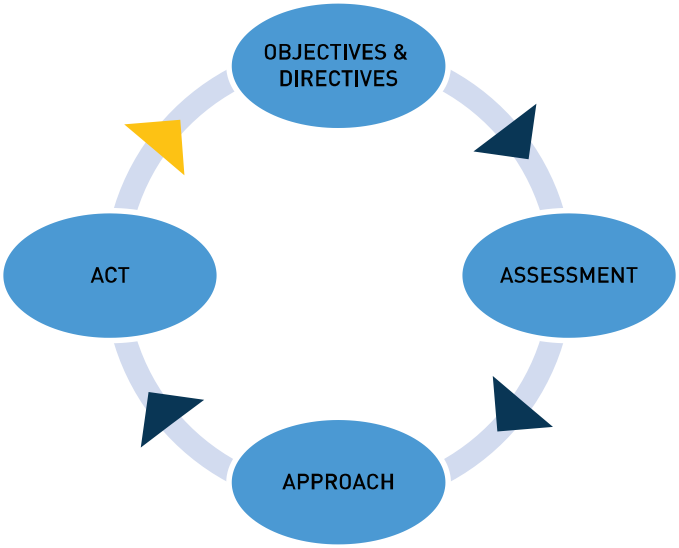


Figure 10 – Strategic cycle

The second concept is assessment which determines the current position of the company. Assessment variables such as the maturity on risk governance of the company in correlation to its current activities support the company in determining the current position in relation to their cyber risk landscape.

These conceptual steps involve a strategic approach. Defining how the organization is realizing its objectives and directives towards protection against cyber related risks based upon the assessment of the organization. The approach needs to be aligned with the organizational business processes and incorporated in the enterprise risk management processes.

The final concept is act, which enables the execution of the defined strategy. This enables the cycle depicted in the CRG framework (Figure 9) which represents the *act* component in the strategic cycle. The yellow arrow is indicated as a new initiation of the cycle based upon new knowledge or activities gained from the CRG framework.

4.6 Continuous approach

Maintaining a continuous approach is an important factor of cyber risk governance as it is not a one time achievement. A top down approach implies developing a strategy (4.5.2) which translates into policies and processes for the guidelines set in the CRG framework (Figure 9). These parts are interrelated and cover an equal motion of gears turning (Figure 11). The turning speed on operational level is considerable higher in comparison with the higher levels. A strategy evidently has a longer expiration date in comparison with activities on operational level.

Continuously on short interval the main operational concepts described in the CRG framework define the concepts which govern risk. The strategic and tactical is depending on slower iterations which are less influenced by the vastly chancing environment on operation level. For the sake of simplicity and maintaining a clear overview the tactical level is incorporated in the operational level starting from the idea that each concept of the operational part is support by policies. However one could interpret policies to be on strategic level.

Figure 11 - CRG framework in motion

Figure 11 defines a top-down motion starting from strategy downwards via the different levels. However sudden developments on operational level can initiate a reversed motion of the framework. New threats can emerge or existing policies are not sufficient enough to define an effective response against risk which is noticed on operational level. This new knowledge could possibly influence the existing policies and strategy of an organization. The knowledge gained on operational level can initiate a bottom-up approach affecting the existing policies and strategy. Therefore in the strategic cycle (Figure 10) of the instrument a yellow arrow is incorporated indicating a new iteration which origins from operational level. Both direction of movements enables organizations to prepare themselves (top-down) against risk as well as act on a changing and dynamic risk environment which is impossible to notice on time from higher levels in the organization (bottom-up).

4.7 CRG framework example cases

The CRG framework (Figure 9) and meta-model (Figure 8) provide an executive auxiliary tool for managers to enable a cyber risk governance strategy in the organization. The model is presented on a high level which implies that no processes are provided in detail. The tool provides guidelines which supports organizations on assessing the situation and incorporating the right characteristics for implementing a strategy and determining the necessary processes. Organizations are free in determining their own strategy, policies, procedures and processes given the tool for governing their cyber risk landscape in implementation in their own organizational structure and culture.

This paragraph describes two simplistic examples of cyber related risks and how to govern these risks via the framework provided (Figure 9). It does not describe the approach and processes in detail and will not be applicable in real world situations, however, it describes the overall high level thoughts of using this model for different cases from a managerial perspective. It does not focus on the technical solution but on the coherence of people, processes and cyber.

4.7.1 BYOD

Bring Your Own Device (BYOD) is one of the recent developments where companies allow employees to user their own laptop and smart-phone to connect to the business IT domain. It is an attractive solution for employees as well as organizational in terms of costs. Nonetheless BYOD enables new IT related risks which should concern organizations. If an organization decides to implement a BYOD program, the tool can be used for constructing a top down plan.

It starts with the construction of a strategic plan for implementing BYOD in the organization as presented in paragraph 4.5.2. Defining clear objectives (e.g. only peripherals can have access after a secured authentication process and is followed by an encrypted and secured connection) followed by an assessment (what are the possibilities for employees in the current state and what in the desired state) will lead to an approach on how to implement the strategy within the organization. In this case for example: which employees are involved and what are the responsibilities on reaching this goal? If the strategy is defined and incorporated in the business processes the actual implementation of the strategy on lower levels in the organization can be started. This initiates the use of the CRG framework (Figure 9).

The strategy is translated into organizational policies and processes which support the activities on operational level for the main concepts as defined; risks, resources, response and reputation. Table 11 provides an overview on translating the different concepts to the implementation of BYOD in the organization and possible questions which would possibly erupt while using the CRG framework.

BYOD implementation – CRG framework		
Main concepts	**Sub concepts**	**Description**
Risks	Threats	Identify the risks directly facing with the use of BYOD e.g. no direct control on the peripheral. Or how do we protect the information?
	Vulnerabilities	Identify the vulnerabilities. What if an employee lost his smartphone which connected to the network?
Resources	IT Resources	Sufficient technical resources are needed to protect the cyber domain against possible risks.
	Funding	Employees should have the right knowledge and skills to safely work with BYOD. The organization should invest in training the employees.
Response	Awareness	The organization should be aware of possible risks. Complete safety cannot be guaranteed so continuous awareness should be present.
	Assess	Continuously assess the situation. Is it safe enough? Do we have the necessary steps taken? Are there new developments?
	Detect	If there is something wrong, detection should display any illegal access or strange behavior.
	Approach	If something is wrong an effective approach needs to be introduced. If an employee lost a smartphone or laptop it should be remotely blocked.

	Responsibilities	Employees are responsible for the safe use of their peripherals on the network. The IT department is responsible for a secure and up to date environment. How responsibilities are arranged if third parties are involved?
	Partnering	Are there best practices for implementing BYOD? What are experiences from other organizations upon which we can learn?
Reputation & assets	Information theft IT Sabotage	In conclusion the analysis of the risks in combination with sufficient funding and the construction of an effective response should contribute to the prevention of information theft and IT sabotage.

Table 11 - Example case BYOD

Again this is a briefly described and high level example, nonetheless the tool is provided to support managers on different characteristics to take into consideration when new IT developments are embedded in the organization.

4.7.2 Unknown targeted attack

In this example the organization is subjected to a new and unknown targeted attack against the cyber domain of the organization. In this situation a bottom-up approach is started since the attack is detected on operational level. An effective response depends on multiple variables in this situation, e.g.: are protocols already defined? Is the detection of the threat on time? Are there best practices in the organization? There are many organization specific scenarios which could occur. Acceptance of these possibilities by the organization increases the awareness which contributes to more mitigation and protection against cyber related risks. Table 12 provides an overview on translating the different concepts to the detection of an unknown targeted attack against the organization and possible questions which could possibly erupt while using the CRG framework.

Unknown targeted attack – CRG framework		
Main concepts	**Sub concepts**	**Description**
Risks	Threats	Identify the attack. How can the threat be stopped or mitigated?
	Vulnerabilities	Are there vulnerabilities which contribute to the attack? A possible assessment of vulnerabilities is needed.
Resources	IT Resources	Provide technical resources to stop the threat, keep the information secure and prevent the attack from happen again.
	Funding	Do we need to invest more time in making the cyber domain more secure or do we need to educate employees?
Response	Awareness	Awareness is a crucial factor for identifying possible threats on time. In the case of an unknown targeted attack awareness introduces a faster response which mitigates possible unwanted outcomes.

	Assess	Assess the situation. Why are we the victim of an attack? Is there a gap in the IT infrastructure which makes it more interesting for unwanted intruders?
	Detect	Next to awareness detection is a crucial factor for identifying possible threats on time.
	Approach	Is there a policy how to cope with this threat? Can we directly stop the threat?
	Responsibilities	Who is responsible for this threat? Is the IT department up to date? Was it a human error? Questions should relate to e.g. the IT department in order to learn and prevent future threats.
	Partnering	What can we learn from other parties coping with these kinds of attacks? Are there best practices?
Reputation & assets	Information theft IT Sabotage	An effective response influences the reputation and assets. Is business continuity maintained? Is information kept indoors?

Table 12 - Example case unknown targeted attack

In this case the approach is depending on the preparation of the organization and how they managed to protect their reputation and organizational assets. In addition this case could lead to new insight within the organization and a push on higher levels to change the strategy of the organizations based on the knowledge gained from this case.

4.8 Validity

The next chapter (chapter 5) will describe the evaluation and validity of the results of this research. The improvements gained from this section which directly influenced the visualization of the tool are briefly discussed in this paragraph.

A meta-model of the framework was introduced as the framework itself (Figure 9) was insufficient in indicating the boundaries of an organization in relation to third parties. Subsequently the framework needed improvements on naming different characteristics of the main concepts. In addition the purpose of the framework is more emphasized on the fact that it provides guidelines instead of actual processes, in addition the CRG framework is only focused on cyber processes in the domain of the own organization. It is an isolated tool on cyber risk governance which does not incorporate the primary processes of an organization. These remarks contributed to changes in the instrument initially presented.

4.9 Retrospect

The tool presented provides an overview of supporting organizations to govern their cyber risk strategy as well as focusing on the operational tasks. This combination of best practices provides an executive instrument which enables a structured and integrated approach for governing risks. The construction of the tool contributes in answering the third and final research question.

RQ 3: How can an executive instrument be developed that contributes to integrally govern cyber related risks within organizations in order to secure information processes as well as IT infrastructures?

The main contribution of this executive instrument is threefold. First, it supports organization in defining a strategy for coping with cyber related risks. Second, it contributes on operational level in mitigating and preventing unwanted consequences of potential risks. Finally this tool provides guidelines which make the use applicable for many companies and organizations. The cyber risk strategy can be shaped or adapted to fit the individual organizational processes and culture.

Integrated governance for cyber related risks within organizations is created by maintaining an integrated view on cyber. Processes, information and technology are the focal point of view and every concept or task is individually related. Securing information processes and IT infrastructures are directly related towards the integrated view on cyber and are in addition absorbed by the four main concepts of the framework; risks, resources, response and reputation and assets.

The framework transcends the boundaries of the organization to actively work on partnering with third parties. Organizations are often involved in a software ecosystem of different sub-contractors. Important is to partner with these organizations in order to share knowledge and jointly mitigate the risk of cyber related threats.

In conclusion the cyber risk governance tool provides a top down executive view and approach which congruence people and IT working seamlessly in order to protect the organization against potential cyber related risks.

5 A first validation of the CRG framework

The evaluation and validation phase of this research is done by conducting multiple semi structured interviews with experts in the field (Table 13). All interviews are transcribed and prepared for content analysis. Content analysis is a highly flexible research method as well as a systematic and rigorous approach to analyze documents in the course of research to generate findings and put them into context (White & Marsh, 2006). The first paragraph describes the outline of the conducted interviews subsequently followed by describing the method used and steps taken for conducting the qualitative content analysis. Finally the results are presented of the findings from the analysis of the interviews.

Expert	Position	Company/University
Expert 1	Professor VU University	VU Amsterdam
Expert 2	Country Security Officer	Atos
Expert 3	Security Principal, Technology Risk IT & Risk Professionals	Atos
Expert 4	Global Portfolio Manager	Atos
Expert 5	Head of Global PHT Defense and Security Portfolio Management	Atos
Expert 6 **(input via Expert 5)**	Vice President Government Affairs Europe and Africa Atos Global PHT	Atos
Expert 7	Cyber Competence Lead IT & Risk Management	Atos

Table 13 – Validation expert interviewees

5.1 Outline interview

All conducted interviews were scheduled in advance and are in conjunction with the preliminary observed research results. The expert interviewees received the research results in advance in preparation for the interview. The interviews started with an introduction regarding this research (such as research method and preliminary results) to the interviewees. The actual starting point of the semi-structured interviews (DiCicco-Bloom & Crabtree, 2006) was the initial constructed CRG framework. Several predetermined open questions (Appendix C – Expert validation interviews) related to the framework where used as guidelines for the interview. These open-ended questions relate to the completeness, correctness and consistency of the constructed framework as well as the practical applicability of the framework. These predetermined questions were supplemented with other questions emerging during the interview. The open questions allowed the interviewee to answer the question base upon own experience. In addition to discussion of the presented framework all experts gave input on the elaboration of this research. The individual conducted interviews took approximately sixty to ninety minutes to complete and were digitally recorded.

5.2 Content analysis – Interview Transcript Review

The multiple interviews are analyzed with the method of qualitative analysis of content emphasizing on an integrated view of speech/texts and their specific contexts (Zhang & Wildemuth, 2009). This method consists of several procedures of processing data supporting valid and reliable inferences. It supports validating the model on its completeness, correctness and consistency. The steps of the method taken are briefly described.

Categories
Cyber
Risk
Resources
Response
Reputation & assets
Governance
Partnering
Strategy

Table 14 - Coding categories

The first step is to prepare the data by transcribing the speech files recorded during the interviews to plain text. The verbalizations are transcribed literally to include all thoughts from the interviewees in order to maintain the context of the interview (Appendix C – Expert validation interviews). In addition a complete transcript is the most useful to compare with other transcripts. The first step is followed by defining the unit of analysis. The main unit of analysis is the CRG framework in combination with the underlying research which was occasionally used for analyzing the validity of the framework. The third step is to define categories and a corresponding coding scheme. Based upon the framework an initial list of coding categories is generated (Table 14). After testing the coding scheme all interview transcripts are coded according to the coding scheme. In addition the transcripts are assessed again to verify the consistency of coding. Based upon the coded text the verbalizations are grouped regarding their category and analyzed to draw conclusions derived from the data. This is done by inter alia looking at relationships between categories and uncovering patterns. In addition the computer program ATLAS.ti is used at the full data set to analyze the recurrence of different concepts in relation to the coding scheme. The next paragraph describes the final step of the qualitative content analysis which is reporting the findings of the conducted interviews.

5.3 Semi structured expert interviews results

The results of the interviews are elaborated and presented based upon individual verbalizations which categorized as described in Table 14. In addition the results are compared in correlation with the analysis section of this research as well as the instrument created. The latter part of this paragraph describes the overall validation and the main noticed suggestions of improvement for the tool.

5.3.1 Risk

The concept risk is a predominant and influential factor which drives the pivotal movement as presented in the CRG framework (Figure 9). All experts confirm that risk is a complex factor which often is underestimated by people. Millions Lines Of Code (LOC) contribute to more complexity and increase the vulnerabilities of software. In addition new areas of vulnerabilities occur due to technical innovations. This makes testing of software more difficult as well as the reproduction of possible bugs. Organization can protect sufficiently against the 'low hanging fruits' or easy access vulnerabilities. Firewalls and virus scanners are in this case supportive but can give a false sense of security. The real targeted attacks are much more complicated and hackers are likely to find possible vulnerabilities in the cyber infrastructure. Nowadays hackers are becoming smarter and have the use of more resources.

All experts claimed increasing risk and complexity with multiple connected organizations. Organizations are interwoven with third parties for managing their cyber. These cyber ecosystems, consisting of multiple stakeholders make it more difficult to define responsibilities and strengthen to deter threats. This makes for an interesting question if organizations nowadays are ready to connect their critical cyber infrastructure and processes. The connectedness of systems also may increase

risk. As users often use the same password and username combinations a hacker can use same datasets on multiple systems.

Important to incorporate in the tool as mentioned by the experts, is the complexity of risk nowadays and the importance for organizations to understand possible risks. Awareness is correlated to risk which triggers an effective and continuous approach for protection against risk and mitigate the outcomes. The results of the interviews emphasize on a clear view on risks in the tool to highlight the importance striving to make organizations aware.

5.3.2 Resources

An effective response is depending on sufficient resources, the CRG framework highlights two types of resources which are supported by the results of the interviews. Experts claim that the right funding in correlation with sufficient knowledge, skills, enthusiasm and passion of the employees contributes significantly to an effective response.

Also mentioned by the experts is the burden that organizations still see managing security. It does not contribute to extra functionality or money which makes the consideration of organizations to actively manage their cyber risk landscape difficult. As one expert explained; "*The right funding and legislation is lacking at the moment. There is a clear governance problem resulting in organizations to depend on the passion and professionalism of employees*".

In addition organizations are short on resources. Finding educated people with the right skills is tough as the knowledge is lacking nowadays. Nonetheless organizations do want to participate in new innovations such as cloud computing or BYOD. However, they are as a result, lacking in knowledge and so increasing possible vulnerabilities of their cyber.

5.3.3 Response

An effective response is, in addition to sufficient funding, depending on the awareness of the organization, organizational awareness and individual awareness by employees as presented by the CRG framework. Common understanding regarding potential cyber risks the organization is facing as well as incorporating cyber risks in the processes of the organization is important for an effective response. All experts mentioned that organizations should under no circumstances exclude their organization for possible attacks. One of the experts suggested visualizing in the tool that once something occur, an organization derives the right conclusions from it. Was it just an incident, or was the policy not sufficient enough? The response of the organizations should incorporate a feedback moment.

One expert mentioned that responding to potential threats is not solely a technical issue, but also related to processes. Encrypting critical organizational information, as well as Principle of Least Authority (POLA), which handles the minimum amount of authority for users entering the system, provides an example. In addition responsibility is an important factor for arranging effective response measures against threats.

In addition the expert claims that software also plays an important role in an effective response. More developments will focus on preventive detection methods. Detecting attacks in an early stage as well as detecting abnormal behavior of the cyber environment contribute to an early detection of threats as well as responding on these threats.

5.3.4 Reputation & assets

Protecting against risks is to maintain reputation and critical business assets of an organization as presented in the CRG framework. Experts mentioned that it is for organizations important to emphasize in the tool on reputation and assets. It supports by created a common understanding on the actual risk organizations are facing. The instrument should also be clear in the fact that it is not solely to damage on cyber level. Other important business factors are also affected such as reputation and business continuity. These are important factors on which organizations derives existence.

5.3.5 Partnering

In addition to the four main components pivoting around cyber, partnering is also chosen as category of interest for the analysis of the interviews. It is important to understand that nowadays governance is not solely dedicated to the individual organization. The organizations are outside its boundaries dependent on other organizations skills and knowledge in the cyber ecosystem. The question is how to arrange responsibility in a chain of organizations and how to assure the responsibility across the whole cyber ecosystem?

One expert mentioned that partnering nowadays is more common in large business sectors. As an example banks in the Dutch financial sector arrange informal meetings to act as a sector against cyber related risks. Organizations are interested in these meetings however reluctant when meetings are heading formal.

Multiple experts claimed that it is important to depict within the tool that protecting an organization against cyber related threats is not solely subjected to one organization. A chain of partners are responsible for shared governance.

5.3.6 Strategy

A top-down approach implies defining the right strategy for an organization to protect against cyber related risks which drives an operational approach achieving the developed strategy, as claimed by multiple experts a reversed motion (bottom-up) is also possible. The strategy could possibly be influenced by the operational activities. On operational level the knowledge is present, business processes are daily influenced by outside threats. As the operational cycle is short cyclic, possible influences and knowledge gained via these activities could possible influence the strategy.

Still, organizations are lagging behind on strategic level. On operational level the cycle turns much faster in comparison with the strategy cycle. Cyber risks should penetrate through management layers of an organization, which is still difficult. As one expert explained; "*The CISO (Chief Information Security Offer) of company X reports back to the CFO (Chief Financial Officer). However security is not a CFO responsibility, but a CEO (Chief Executive Officer)*". There is a main focus on technology which

is currently heading technically in the correct direction. However, we are also talking about people and processes which tend to be much more difficult to govern.

5.3.7 Governance

Managing the technology does not uncover the main challenges nowadays. The emphasis is on governing processes and people, which is proven to be far more complex, as one expert claimed. Models rely on controllable goals, or a top-down strategy. In practice this is not always the case. Processes on operational level influence the strategy of an organization. These directions are also incorporated in the model as the depicted turning gears can operate in twofold; top-down and bottom-up.

One expert defined in general two types of governance: organizational governance and ecosystem governance. Forcing a top-down strategy is possible by defining a new top of collected governance. Establish governance between all the stakeholders in the ecosystem. Or a top-down approach with the use of (open source) software which can be controlled and maintained within the organization, which entails the right knowledge and skills.

5.3.8 Practical applicability

One of the main concerns for developing the tools is practical applicability. How can managers within an organization use this tool for their own benefit, in order to protect themselves against cyber related threats. One of the experts emphasizes on the coherence between cyber, processes and people which the tool should represent. Each component within the tool should be shortly elaborated creating a clear repository which provides insight for managers on each individual concept. In a subsequent step these repositories can be transformed to milestones which can act as a checklist, improving the practical applicability. To make the tool even more comprehensive best practices could possibly be incorporated to represent the applicability of the model.

5.3.9 CRG framework

In conclusion the initial constructed framework was positively received by the interviewed experts, referring to the concepts presented in the framework. The statements of the interviewees corresponded overall amongst each other en no remarkable differences where mentioned during the interviews. However, several elements of the tool were suggested for improvement based on their own experience or (practical) vision in the field. The most discussed points are collected and described in this paragraph.

Noticeable during the interviews were the different views regarding the framework; for instance a security expert had a different view in comparison with an expert on the field of risk. This is illustrated via the following example: the tool does not make a difference between incident management and risk management when looking at approach. Assuming an approach to protect, mitigate, defend or deter, the framework does not make any distinction in type of approach. As the framework aims for generalizability the type of approach is not the main focus of the framework. Organizations are free in the type of approach and possibly adapt multiple approaches (e.g. mitigate and deter). In avoidance of complexity, maintaining a clear overview the framework emphasizes solely on a high level approach for managers to take into consideration.

The next item noticed during the interviews is the stratification of the framework. The framework takes the three layers of strategy, tactical and operations as starting point. The initial framework did not depict these different layers sufficient enough. In addition the operation and tactical loop were as well not visualized in a clear and understandable way. The research results presented the different layers, however were not sufficient depicted in the framework itself. Suggestions were made for an extra high level model of the CRG framework to include this aspect of multiple tiers and how these correlate with the framework, as well as incorporate the tactical level which needed to be clarified. This makes especially sense when representing the cycle interval of each individual loop (operational – high, tactical – medium, strategic – slow). However in the final version of the instrument this stratification is touched, however not explicitly mapped to operational, tactical and strategic level as these layers could possibly be differently interpreted and viewed.

Improvements were also suggested on the naming and ordering of different concepts presented in the framework. The initial strategy loop incorporated in the framework consisted of the concept 'governance' which obscured the actual meaning of incorporating operational activities in the model. The framework in itself represents cyber risk governance. In addition an expert suggested changing order of 'governance' and 'approach' in the strategic cycle. First determine the guidelines followed by the approach. Possibly this suggestion is due to naming of the concept. Important is to develop an approach of implementing the strategy within the organization, this by incorporating the strategy in the enterprise risk management, or regular business processes of an organization.

An important issue which rose during the interviews was the question when the model transcends the boundaries of an organization. The initial model represents the governance in a single organization transcending the boundaries via 'partnering' and 'responsibilities'. However in the view of the experts this was not sufficient. Nowadays organizations are involved in collected governance as they are operating in a cyber ecosystem. The tool should emphasize on the possibility of multiple governance structures when managing risk.

Final factor of improvement makes the exact purpose of the tool clear. Possibly due to the naming of the concepts, the purpose of each concept within the tool was obscured. One expert was thinking in processes at each concept of the framework, which confused his vision. In the model not every concept is depicted as a process, hence the framework defines guidelines not solely processes. Two types of processes were mentioned: the cyber processes which protect the cyber of an organization, and the primary processes of an organization. These two processes where intertwined in his vision. The suggestion was to keep the model completely in the cyber domain. Initially this was the purpose of the framework, but as mentioned not sufficiently depicted.

The outcomes and suggestions as described above were used to improve and validate the cyber risk governance framework. Visual improvements were made to make the model more understandable and clear. In addition a high level meta-model is created and introduced to emphasize on the stratification of the framework and making the organizational boundaries more clear.

6 Conclusion

This chapter will provide an answer to the main research question in combination with a recap on the sub research questions. In addition a definition of Cyber Risk Governance (CRG) governance is given as it is not defined yet in scientific literature. Therefore this research proposes the following definition of CRG: "*Cyber risk governance refers to protection against cyber related risks and aims to mitigate unwanted consequences by coordinating activities between human, processes and IT assets".*

The main goal of this research is constructing a managerial tool for organizations to protect themselves against cyber related risks. This is done by supporting the establishment of integrated governance within an organization, not only by focusing on cyber but also on people as well as on processes. The following research question was formulated in order to answer it by means of this research:

How can organizations manage cyber related risks in such a way that integrated governance is established in addition to securing IT infrastructures?

In order to answer this main research question the three formulated sub research questions answered previously in this research are briefly recapped providing an overview of the answers to the sub research questions.

RQ1: What are the current views in literature on establishing integrated governance for protecting IT assets?

The literature taught us that the cyber risk landscape is a complex, dynamic and unpredictable environment which evolves rapidly forcing organizations to take effective measures. As every organization is unique in its context, culture, business processes and IT assets which make it impossible to define one silver bullet solution to protect organizations from cyber related risks.

Instead of searching for unilateral solutions, one should define guidelines for organizations to govern their own cyber risk strategy. An influential factor facing risk is organizational awareness and attitude. Organizations should be aware of a continuous threat landscape which is rapidly evolving and successfully affecting organizational assets and reputation. Knowing the potential threats feeds the organizational awareness to continuously assess the cyber strategy. Cyber risk governance should be incorporated in the DNA of an organization to ensure an effective and integrated approach.

More meaningful is to understand that humans are a leading factor in managing cyber related risks. Not solely the technology needs the attention, a broader perspective of people (skills and knowledge), processes and technology is desired. An effective approach consists of continuous assessment of cyber related risks, attack potential threats and vulnerabilities and mitigate outcomes of potential threats in order to protect IT assets. Not solely the information security perspectives (confidentiality, integrity and availability) are at stake but also the critical business (IT) assets and reputation.

Conclusively establishing an integrated governance approach for protecting IT assets is based upon multiple factors and dependencies. Main focus areas which attract the attention are awareness, understanding the complexity of the cyber landscape, maintaining a continuous approach and providing sufficient resources are the key elements for an integrated approach.

RQ 2: What do we see in practice with regard to cyber related risks influencing organizations in managing IT infrastructures?

The practical view on cyber related risk taught us the evolving complexity of IT nowadays. This makes it difficult to manage IT assets through all layers of an organization. Making the right (top down) decisions encompasses the right knowledge, skills and sufficient resources which is lacking or not present within the different layers of an organization. Managers cannot take decisions if they are not aware or familiar with the problems of a changing cyber risk landscape.

In essence two types of possible outcomes regarding to cyber related risk can be defined when IT assets are compromised: information theft and IT sabotage. Those two outcomes have significant influence on the organizational reputation and business processes (e.g. business continuity). These outcomes should have a positive influence on the awareness and attitude of organizations referring to manage their protection. However, the invested cases and the practical view taught us that amongst organizations there is still an improper attitude showing a lack of awareness and disregarding responsibilities in protecting their cyber domain. Organizations still see managing risks as a burden: appeals for investing money, however, it does not directly bring a return on investment (ROI).

The complexity of more organizational structures is also part of the problem. Many organizations rely on third parties for managing their cyber infrastructures. Bringing the critical infrastructures to other parties implies multiple governance structures, making it more complex to define the individual responsibilities.

RQ 3: How can an executive instrument be developed that contributes to integrally govern cyber related risks within organizations in order to secure information processes as well as IT infrastructures?

As the cyber risk landscape is becoming more complex, the quest for a solution is a daunting task. This research aims at constructing an executive and practical instrument giving managers structure, insight and knowledge on carrying out protective measures against cyber risks. It provides an overview on the key elements which needs to be taken into consideration. In addition it emphasizes the fact that governance transcends the organizational boundaries and is possibly affected by the governance of third parties.

The proposed tool in this research contributes to formulate a strategy and translate these into operational activities for protecting the organization to their particular cyber threat landscape. The tool provides guidelines which make it applicable for multiple companies and organizations to use

the model. It supports organizations to establish integrated governance by not solely focusing on IT but also on people and processes.

The proposed cyber risk governance tool provides a managerial view and approach which congruence people and IT working seamlessly, in order to protect the organization against potential cyber related risks.

How can organizations manage cyber related risks in such a way that integrated governance is established in addition to securing IT infrastructures?

Combining the results of the sub research questions to the main research question concludes to the result that it is possible for organizations to manage cyber related risks maintaining integrated governance. However organizations are bound to certain characteristics which need to be taken into consideration as they influence the result of successful governance. In addition they are possibly limited by external forces which affect the control mechanisms of an organization.

To support answering the research question a hands on managerial tool – the cyber risk governance Framework (Figure 9) – is developed which supports organizations in protecting the organization against cyber related risks. It supports the development of a strategy and arranging the cyber risk governance of the organization amongst risks, resources response and reputation and assets. Addressing these main elements in the framework provides managers with the key concepts on how to react on a changing cyber threat landscape and maintaining integrated governance to ensure a safe organizational cyber domain. The rapid developments of IT and changing cyber risk landscape compel organizations to actively and continuously assess their critical cyber infrastructure in order to create an effective response. Organizations need to address the correct attitude and organizational awareness to manage their cyber risk landscape. Managing cyber in organizations requires a more broadened view from information technology extended to processes and people. The proposed tool in this research supports managers to organize and control the cyber domain of an organization by describing the main concepts and key characteristics of controlling CRG regardless the type of business or organization.

There are certain limitations in answering this question positively. When an organization is depending on third parties in a chain of organizations (cyber ecosystem) and cyber is outsourced to these organizations it will lead to collected governance structures. In other words: the organization is depending on the governance model(s) of other organization(s). This transcending governance outside the organizational boundaries results in additional challenges and possible loss of control. The proposed tool takes this cross boundary governance into consideration; however, as an organization it is of importance to understand the implications with involvement of third parties and the effects on their own cyber governance structure.

The most important factor of a successful cyber risk governance implementation is the benevolence of an organization. This by means of investing and funding through al layers of an organization, for an effective approach and maintaining a correct attitude (awareness) of the possible risk facing. Organization should provide sufficient funding (e.g. money, time or managerial and executive

support) in order to support the activities on CRG. In addition investments on knowledge and skills of the employees are necessary for an effective approach. Organizations are reluctant to invest in activities which do not provide a direct return on investment. However the dependency on IT to manage the critical business processes nowadays. Knowing possible negative outcomes should organizations convince to actively strive for a secure and safe cyber domain.

7 Discussion

The discussion section of this research will reflect on three different issues. First a reflection is given on the research which uncovers challenges during this research and how this challenges where coped with. Subsequently the internal and external validity of the research is addressed. The final paragraph focuses on describing the limitations of this research.

7.1 Reflection

Prior and during the period of this research it became clear that the field of cyber risk governance is a hot topic both in the scientific and practical world. The results of the interviews and study made clear that there is a substantial scope for doing extensive research. This was also supported by the many cases regarding cyber security which made the Dutch and international news and underlies even more the importance of research in this field.

Current studies, methods and literature are well prepared on describing the technical and process side of cyber risk governance. Nonetheless the constructing of a high level view on cyber security including technology, processes and people is not yet been done scientifically. The freedom of movement and amount of topics in this research domain made scoping this research challenging. The challenge at first hand was creating a scope with a high level view preventing turning into a vague and oversized perspective.

Another challenging factor in this research domain is the many ‘unknowns’. Definitions are not yet well covered or adapted by science and the cyber domain is in certain cases a big question. The fast evolution makes it a highly unpredictable environment therefore sometimes hard to determine or grasp different situations or problems, such as cyber threats. Uncovering these grey areas and describing these areas from a high perspective unchallenged certain unknowns and made them possible to include into the research.

One of the main objectives is creating a tool which enables managers in organizations to manger cyber related risks. Combining the practical utility of this tool in combination with science revealed new challenges. Scientific and social contribution are both important however challenging to combine these purposes in one tool. And in many cases the real world is behaving differently in comparison with literature and suggested results. For example this research initially strived for a top-down strategy, which is in the proposed situation desirable, however in practice not the case. Developments in the cyber domain force a bottom-up strategy where operational activities influence the strategy of cyber risk. Initially this approach is not incorrect, however does illustrate a force which cannot be controlled within an organization, even not with a model.

Finally the interviews with the expert were of great value for this research, however posing some challenges. An expert on security presumes a different view on certain concepts in comparison with an expert on risk. This is also influenced by their working environment or previous positions. For example some experts had a background in defense, which created another view on the level of policies in an organization. As literature suggests policies are on tactical level, the expert positions policies on strategic level. Possible influence by background, the maturity of research in the field and

the many grey areas made it challenging to combine the information and position it in scientific context.

7.2 Validity

The internal validity of this research was affected by the scientific data collection. As mentioned in the introduction, scientific research on this particular field is scarce. Dependency on grey literature increased, which concerns the validity of the gathered information. The use of different renowned sources in addition with expert input made for more reliable and trustworthy sources. In addition the literature review and practical view are compared and analyzed, validating possible gaps or structural differences between the main sources of this research.

External validity is ensured by maintaining a broad perspective on the target group as well as describing cyber risk governance from a high perspective. This view results in a tool which is generalized for many organizations and purposes. This makes the tool applicable in scientific context as well in a social context. Due to a continuous view on the real world increases the applicability of the tool in a practical manner.

7.3 Limitations

During the preliminary phase of this study it became clear that the field of cyber risk governance is a new research area which is not yet discovered by scientists holding many grey areas. Scientific research in this field is scarce in comparison with the work that is already done by research institutes and (consultancy) companies. At first the start of this research was characterized by finding useful documents and material which could be incorporated and contributed in an objective and scientific manner. Therefore the preliminary phase of this research was depending on the input of the experts participating in this research.

The dynamic and vastly changing environment of cyberspace affected the writing. Even during this research new developments were influencing certain sections. The observance of these developments made clear that not every accomplishment in the cyber domain can be incorporated in this research. Therefore this research aims at incorporating as much possible recent developments maintaining the most actual view nonetheless not focusing on minor details. The writing aims at a higher perspective on developments making it more readable in the near future.

The preliminary phase had its aftereffects on the course of this research. More time and resources were used to construct a solid and scientific base to build on. This resulted in the construction of a cyber risk governance framework which was validated by multiple experts in the field. The time intensity of these different activities making the actual practical implementation of the framework via a case study fell due on time constraints.

Regardless these constraints and concessions made, the attempt of researching cyber related risk in perspective of integrated governance was maintained. The input from the experts based upon their practical knowledge and understanding of contemporary risk on organizations including the result yielded from the preliminary phase of this research made a combination of scientific and practical

views. The result of the cyber risk framework aims not solely on practical use, but provides also a clear overview for scientists in the cyber risk domain.

8 Future research

The research domain of cyber risk governance provides ample opportunities for future research. The first opportunity is to extend this research from single organizations to 'chained' organizations in a cyber ecosystem. As this research touches the implications of operating with multiple organizations in a cyber ecosystem, it still provides many areas to explore scientifically. This is seen in terms of responsibilities, dependency and partnership. The near future also provides the field of legislation for securing operations. As organizations become more dependent on partnership and outsourcing cyber it will provide many opportunities for further research. This is also the case for many nations which are actively striving for securing their critical and national infrastructures. This research could possibly contribute to discussions on national cyber security.

Subsequently this research can be extended by testing the executive instrument via a case study in multiple organizations. In addition efforts can be made to make the model more practical in use. This can be possibly done by investigating for improving the model in terms of readability and the ease of use.

References

ANP. (2012, March 20). Ruim 300.000 medische dossiers gelekt. *NU.nl*. Retrieved April 27, 2012, from http://www.nu.nl/internet/2791579/ruim-300000-medische-dossiers-gelekt.html

Axelrod, C. W. (2006). Cybersecurity and the critical infrastructure. *Information Systems Control Journal*, *3*, 24–28.

Bakker, J. (2012, March 19). Gehackt KPN zegt sorry. Retrieved April 27, 2012, from http://webwereld.nl/nieuws/109876/gehackt-kpn-zegt-sorry.html

Betz, C. T. (2011). *Architecture and Patterns for IT Service Management, Resource Planning, and Governance.* Elsevier.

Bodeau, D., Boyle, S., Fabius-Greene, J., & Graubart, R. (2010, September). Cyber security governance. Mitre.

Cabinet Office. (2011, November 25). The UK Cyber Security Strategy. Retrieved from http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

CACI. (2011). Cyber Threats to National Security.

Chung, E. (2011, March 27). PlayStation data breach deemed in “top 5 ever.” Retrieved from http://www.cbc.ca/news/business/story/2011/04/27/technology-playstation-data-breach.html

Cooper, H. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge, Technology & Policy*, *1*(1), 104–126.

de Winter, B. (2012, March 27). 17-jarige bekent hacken KPN. *NU.nl*. Retrieved April 27, 2012, from http://www.nu.nl/internet/2773417/17-jarige-bekent-hacken-kpn.html

Department of Defence. (2011, July 14). Strategy for operating in cyberspace.

Department of Homeland Security. (2009). National Infrastructure Protection Plan. Retrieved from http://www.dhs.gov/files/programs/editorial_0827.shtm

Department of Homeland Security. (2011, September). Blueprint for a secure cyber future. Retrieved February 1, 2012, from http://www.dhs.gov/files/publications/blueprint-for-a-secure-cyber-future.shtm

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education*, *40*(4), 314–321.

Essers, L. (2012, February 10). KPN lekt persoonsgegevens 500 klanten. Retrieved April 27, 2012, from http://webwereld.nl/nieuws/109492/kpn-lekt-persoonsgegevens-500-klanten---update.html

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40.

Fox IT. (2011, September 5). DigiNotar public report. *Rijksoverheid.nl*. rapport. Retrieved April 17, 2012, from http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html

Fox IT. (2012, April 21). Spoed penetratietest. Fox IT. Retrieved from http://zembla.vara.nl/fileadmin/uploads/VARA/be_users/documents/tv/pip/zembla/2012/Verzuimpolitie2/Rapport_Fox-IT_VCD_PR120109.pdf

Geers, K. (2011). *Strategic cyber security*. CCD COE Publication.

Georgia Tech Information Security Center. (2011). *Emerging cyber threats report 2012* (p. 16).

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *ACM*, *46*(3), 81–85.

GOVCERT. (2010, November 12). Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010. Retrieved from http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html

GOVCERT. (2011, February 28). De Nationale Cyber Security Strategie (NCSS). Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/28/nationale-cyber-security-strategie.html

Information Security Forum. (2011). Cyber Security Strategies: Achieving cyber resilience. Retrieved from https://www.securityforum.org/downloads/documentview/5901

International Organization for Standardization. (2012, January 5). ISO - International Organization for Standardization. Retrieved February 13, 2012, from http://www.iso.org/iso/catalogue_detail?csnumber=39612

Internet death sentence for DigiNotar's Root CA. (2011, October 29).*Pastebin*. Retrieved April 26, 2012, from http://pastebin.com/SwCZqskV

ISACA. (2012, January 12). COBIT framework for IT governance and control.

IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management 2nd Ed.* (2nd ed.). ITGI.

IT Governance Institute. (2007). *COBIT Security Baseline: An Information Survival Kit, 2nd Edition*. ISACA.

Justitie, M. van V. en. (2011). *Cybersecuritybeeld Nederland*.

Justitie, M. van V. en. (2012, March 6). Veiligheid in cyberspace. Boom Lemma. Retrieved from http://wodc.nl/onderzoeksdatabase/jv201201-veiligheid-in-cyberspace.aspx?cp=44&cs=6797

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies.

Nieuw super spionagevirus Gauss ontdekt. (2012, August 9).*Security.nl*. Retrieved from http://www.security.nl/artikel/42599/1/Nieuw_super_spionagevirus_Gauss_ontdekt.html

Nightingale, J. (2011, September 2). DigiNotar Removal Follow Up. *Mozilla Security Blog*. Retrieved April 26, 2012, from http://blog.mozilla.org/security/2011/09/02/diginotar-removal-follow-up/

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. Presented at the Proceedings of the 5th International Conference on Information Warfare and Security, Dayton.

Ponemon Institute. (2011, August 2). First Annual Cost of Cyber Crime Study. ArcSight. Retrieved from http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

Seidel, J. V. (1998). Qualitative Data Analysis. Retrieved from http://www.qualisresearch.com/qda_paper.htm

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

Takeda, H., Veerkamp, P., & Yoshikawa, H. (1990). Modeling Design Process. *AI Magazine*, *11*(4), 37.

The World Economic Forum. (2012). Partnering for Cyber Resilience.

TNO. (2012, April 10). Kosten cybercrime grotendeels voor rekening van bedrijfsleven. *TNO*. Retrieved April 10, 2012, from http://www.tno.nl/content.cfm?context=thema&content=prop_nieuwsbericht&laag1=897&laag2=920&laag3=115&item_id=2012-04-10%2011:37:10.0&Taal=1

Vaishnavi, V., & Kuechler, W. (2004). Design Science Research in Information Systems. *A journal on the theory of ordered sets and its applications*, *48*(2), 133–140.

van de Weerd, I., & Brinkkemper, S. (2008). Meta-modeling for situational analysis and design methods. *Handbook of research on modern systems analysis and design technologies and applications*, 38–58.

van der Ploeg, P. (2011, September 3). Browsers zeggen definitief vertrouwen in Diginotar op. *nrc.nl*. Retrieved from http://www.nrc.nl/nieuws/2011/09/03/browsers-zeggen-vertrouwen-in-diginotar-op/

Verschuren, P. J. M., & Doorewaard, H. (2007). *Het ontwerpen van een onderzoek*. Den Haag: Lemma.

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: on the importance of rigour in documenting the literature search process, *3*(15), 1–13.

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371–376.

von Solms, R., & von Solms, B. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, *25*(6), 408–412.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future. Writing a literature review. *MIS Quarterly*, *26*(2), 13–23.

White, M. D., & Marsh, E. E. (2006). Content Analysis: A Flexible Methodology. Retrieved from http://hdl.handle.net/2142/3670

Whitman, M. E., & Mattord, H. J. (2011). *Principles of Information Security*. Cengage Learning.

Wiener, N. (1948). *Cybernetics or Control and Communication in the Animal and the Machine*. New York: John Wiley.

Wikileaks. (2012, April 12). Wikileaks. Retrieved from http://www.wikileaks.org/wiki/Main_Page

Wikipedia. (2012a, April 18). Stuxnet. *Wikipedia, the free encyclopedia*. Wikimedia Foundation, Inc. Retrieved from http://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=487015573

Wikipedia. (2012b, April 24). Hack bij DigiNotar. *Wikipedia*. Wikimedia Foundation, Inc. Retrieved from http://nl.wikipedia.org/w/index.php?title=Hack_bij_DigiNotar&oldid=30242446

Williams, P., & Manheke, R. (2010). Small Business - A Cyber Resilience Vulnerability. *International Cyber Resilience conference*. Retrieved from http://ro.ecu.edu.au/icr/14

Winder, D. (2011). Persistent and Evasive Attacks Uncovered. *Infosecurity*, *8*(5), 40–43.

Zembla. (2012, April 19). Honderdduizenden medische dossiers toegankelijk. *Zembla*.

Zhang, Y., & Wildemuth, B. M. (2009). Qualitative analysis of content. *Applications of social research methods to questions in information and library science*, 308–319.

Glossary

Cyberspace
The interdependent network of information and communications technology infrastructures, including the Internet, telecommunications networks, computer systems and networks, and embedded processors and controllers in facilities and industries (Department of Homeland Security, 2011)

Cyber attack
Generally an act that uses computer code to disrupt computer processing or steal data, often by exploiting software or hardware vulnerability or a weakness in security practices. Results include disrupting the reliability of equipment, the integrity of data, and the confidentiality of communications (CACI, 2011).

Cyber governance
The component of enterprise governance that addresses the dependency on cyberspace in the presence of adversaries (Bodeau et al., 2010).

Cyber resilience
The organization's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace (Information Security Forum, 2011).

Cyber risk governance
The protection against cyber related risks and aims to mitigate unwanted consequences by coordinating activities between humans, processes and IT assets

Cyber security
Cyber security is the organization's ability to secure its people, information, systems and reputation in cyberspace (Information Security Forum, 2011).

Cyber risks
The probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation (The World Economic Forum, 2012).

Cyber threat
A potential cyber event that may cause unwanted outcomes resulting in harm to a system or organization (The World Economic Forum, 2012).

Governance
A set of responsibilities and practices exercised by the management (board and executive management) providing strategic direction. This in such a way that the set objectives are achieved, verifying that organizational resources are used responsible and that risks are managed properly (IT Governance Institute, 2006).

Information security
Information security addresses the protection of information, confidentiality, availability and integrity throughout the life cycle of the information and its use within the organization (IT Governance Institute, 2006).

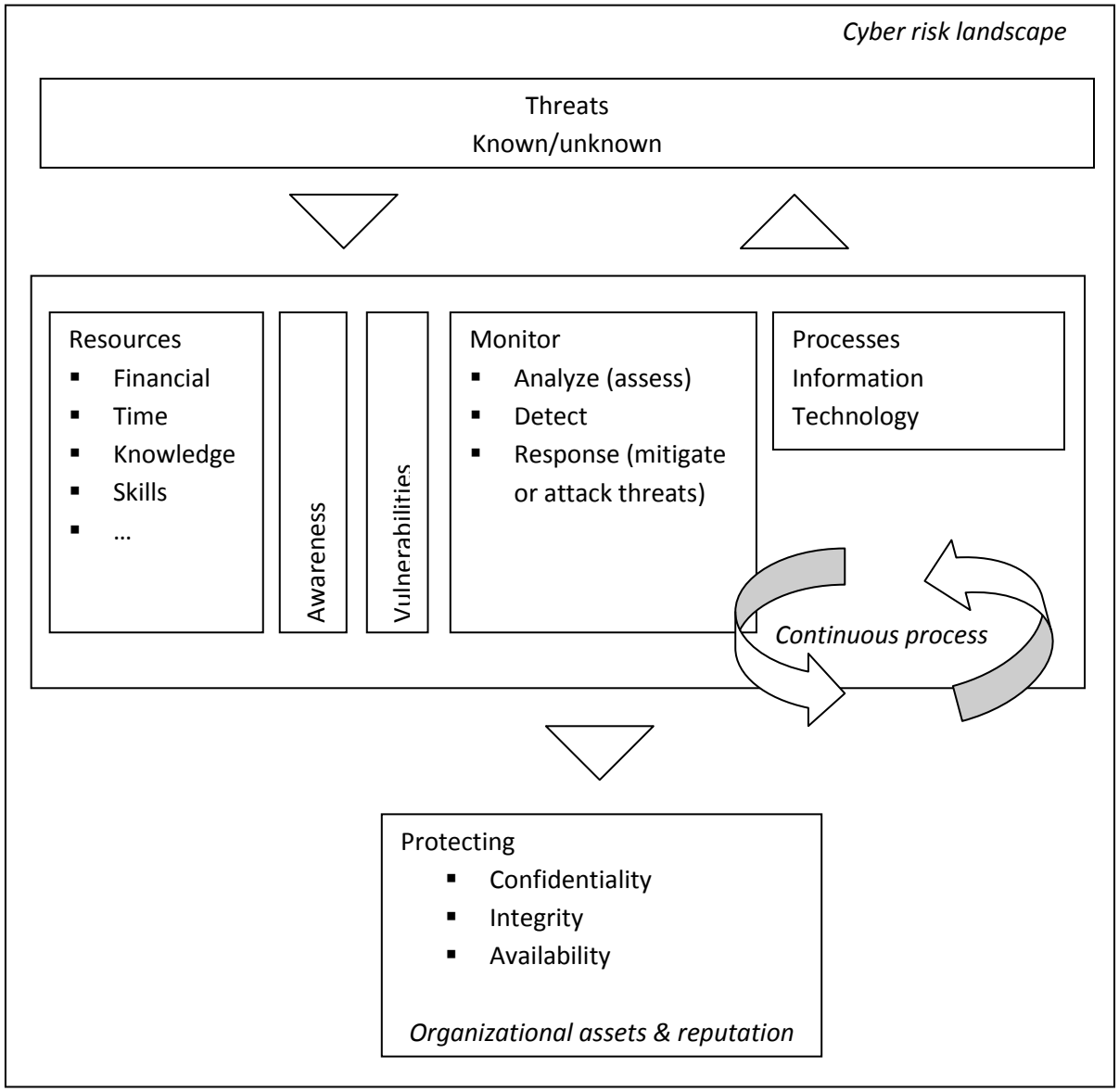
Appendix

Appendix A – Abbreviations

AET
Advanced Evasive Technique 27
APT
Advanced Persistent Threat 27, 48
BYOD
Bring Your Own Device 42, 55
CA
Certificate Authority 36
CEO
Chief Executive Officer 62
CFO
Chief Financial Officer 62
CIKR
Critical Infrastructure and Key Resources 33
CISO
Chief Information Security Officer 62
CSO
Chief Security Officer 39
DoS
Denial of Service 11
ERM
Enterprise Risk Management 28, 34, 48
ICT
Information and Communications Technology 23
IS
Information Science 23
Information Security 25
ISP
Internet Service Provider 27
IT
Information Technology 11
LOC
Lines Of Code 60
PDD
Process Deliverable Diagram 16
PLC
Programmable Logic Controllers 38
POLA
Principle of Least Authority 61
QDA
Qualitative Data Analysis 46
ROI
Return On Investment 66
SCADA
Supervisory Control and Data Acquisition 38
TTP
Tactics Techniques and Procedures 31

Appendix B – Overview cyber risk landscape

The figure below is a conceptual basic overview used to analyzing the cyber risk landscape in chapter 4.



Appendix C – Expert validation interviews

Categories
Cyber
Risk
Resources
Response
Reputation & assets
Governance
Partnering
Strategy

Table 15 - Color codes transcripts

This appendix provides an overview of coded interview transcripts (Dutch). Chapter 4.7 describes the method of analysis and results of these interviews. The interviews were conducted via open-ended questions used as a guideline for the interview. Not all questions were directly asked at the interviewees, in many occasions the answers to the question where interwoven in other answers and input given.

The following open-end questions where used during the interviews:

- Does the framework represent a complete overview of concepts regarding cyber risk governance in order to protect an organization against cyber related risks? (completeness)
- Are the relations between the concepts in the framework presented correct in conjunction with the concepts presented? (correctness)
- Are the framework and its concepts presented consistent? (consistent)
- In what way should this framework be implemented in an organization in terms of practical applicability?
- Are there any other suggestions or improvements regarding this research (presented in the thesis) and presented framework?

The following paragraphs are the coded interview transcripts which are written and elaborated in Dutch. The coding of the transcripts is in conjunction with Table 15.

Expert 1

[*Introductie model. Nadruk van dit interview ligt op risk en de response gezien de expertise van de geïnterviewde*]. Een eerste suggestie is om ook met bedrijven en overheid te praten. Dit is misschien wel belangrijk. Momenteel zijn ze daar heel erg met security bezig. Er is veel sturing van boven. Zij zijn zich rot geschrokken ook vanwege het Diginotar incident. Er is daar nu heel veel druk van boven om dit beter te gaan regelen. Een heleboel van die overheden kunnen dat niet, dus dat zijn interessante cases. In oktober vorig jaar (lektober) had je al die gehackte websites van overheden. Dan zie je dat daar dingen ontzettend slecht belegd zijn. De een die rommelt maar wat aan en brengt zijn website over. En niemand heeft eigenlijk overzicht hoe dat security technisch in elkaar zit. Het is wel aardig om die zaken naast elkaar te zien.

Diginotar is een voorbeeld bij uitstek waarbij de procedures redelijk goed geregeld waren echter de strikte implementatie daarvan wat achterbleef. Het is heel knullig in elkaar gezet; zelfde passwords die overal gebruikt werden. En kwetsbare software waar je niet overheen komt. Vervolgens geen "harde muren" tussen verschillende informatiestukjes. [*Daarnaast zijn er hele basale fouten gemaakt*] **Het klopt inderdaad dat er hele basale fouten zijn gemaakt.**

[*En dat is het frappante. Als je als bedrijf opereert in een dergelijk gevoelige omgeving, met informatie die je moet beschermen met eigen certificaten*]. Het is inderdaad de veiligheid garanderen van die certificaten en daar hebben ze gefaald.

[*Vervolgens is de link gelegd in het framework naar awareness. Men dient de juiste attitude te hebben jegens veiligheid. Hoe creëren we de juiste awareness binnen bedrijven?*]. Het is nu wel zo dat sinds Diginotar de overheid in ieder geval heel erg wakker is geschud. Het duurt natuurlijk wel een tijdje voordat dat allemaal doorsijpelt. [*Ik heb ook het idee dat men eerst tegen een muur moet aanlopen*]. Dat is in Nederland ook een goede wake-up call geweest. En het is sneu voor de Iraniër(s) die daar de dupe van zijn geworden. Voor Nederland is het zeker een goede wake-up call.

[*In dit gesprek wil ik het gezien uw achtergrond graag hebben over de Risk component in het framework. Wat maken bedreigingen zo complex tegenwoordig? Waarom gaat het fout? En wat zou een juiste aanpak zijn? De informatie uit dit gesprek kan ik dan terugschalen richting mijn onderzoek om te kijken of het risico component in het onderzoek voldoende is uitgewerkt*]. Ik kan daar wel wat over zeggen, het is echter niet zo dat ik in alle gevallen daar van wat weet. De organisatie kant ken ik vrij slecht. Het grootste probleem is denk ik toch dat mensen naar software aankijken in structuur gevatte wiskunde. En wiskunde is; het zit allemaal logisch in elkaar en als je het maar goed ontwerpt dat zitten daar geen fouten in. Dus fundamenteel zouden er geen kwetsbaarheden in software moeten zitten. Dat is een misvatting. **Een onderschatting van de complexiteit waar we momenteel mee te maken hebben. De werkelijkheid is dat dit het bevattingsvermogen van mensen te boven gaat en dat geldt voor alle software tegenwoordig. Het gaat over miljoenen regels code.** Daar zitten fundamenteel altijd fouten in. Daar ontkomt je niet aan. Dat zijn fouten van verschillende aard, maar er zitten altijd fouten in. Schattingen lopen uiteen van hoeveel fouten dat zijn. Maar de meest gunstige schatting is een fout of een halve bug per duizend regels code. Meer gebruikelijk is 2 tot 4 tot 16 bugs per duizend regels code. Dat betekent dat je een systeem als Windows met honderd miljoen regels code; ga er maar vanuit hoeveel bugs daarin zitten. Niet alle bugs zijn kwetsbaarheden waar je als aanvaller gebruik van kunt maken maar een percentage daarvan weer wel. Ik heb het over duizenden tot honderdduizenden bugs en dat is enkel nog maar het besturingssysteem. Dan heb ik het nog niet over je Oracle database of alle andere back-ends die men kan draaien. En dat gaat niet weg, daar ontkomen we ook niet aan. Ze zijn van heel verschillende aard en dat is ook niet iets waar je op de langere termijn tegen kunt bewapenen.

Wat voor threats/bedreigen heb je uiteindelijk; je hebt de zogenaamde "low hanging fruits". Waar je als bedrijf jezelf gemakkelijk tegen kunt bewapenen. Daar kun je een firewall of virusscanner en dergelijke voor gebruiken. Maar die geven wellicht toch een vals gevoel van veiligheid. Want waar je dus niet tegen wapent zijn de echt gemotiveerde en technische zeer geavanceerde aanvallen die specifiek op jouw gericht zijn. Dus echt de targetted attacks. Dus als aanvallers bij jou naar binnen willen komen is het onwaarschijnlijk dat ze niets zullen vinden. Dus wat dat betreft is het goed om die awareness te hebben en eventuele aanvallen niet uit te sluiten.

[*Dus in de basis maken aanvallers gebruik van de zwakheden in een system*]. Ja, en daarnaast de goedgelovige medemens die je opbelt en bijvoorbeeld vraagt naar een password onder de noemer ik kom er even niet in. [*En aansluiten de 0-day vulnerabilities*]. Ja, en het rare van deze vulnerabilities

die zijn al een kwart eeuw bekend. Aanvallen die gebaseerd zijn zoals buffer overflows. Deze al gebruikt in 1988. Dat was ook de eerste en enige keer dat het internet uit werd gezet. Dus dat was een zodanig ernstige aanval dat alle machines aangesloten op het internet uitgezet diende te worden. Dus dat is inmiddels behoorlijk lang geleden. En daarvoor werden ze al beschreven in 1972, als mogelijk. Diezelfde kwetsbaarheid vind je nu nog zoals in de aanval op de Iranese kerncentrales (Stuxnet). De Stuxnet aanval maakt gebruik van dezelfde buffer overflow aanval. Hoe kan het dat we al meer dan een kwart eeuw bezig zijn om een heel primitieve bug uit te bannen als aanvalsmogelijkheid? Wij hebben er ook onderzoek naar gedaan of het afneemt. Aanvallen via je website aanvallen via andere dingen. Nemen die percentages van de aanvallen, van een dergelijk oude bug nou af. Dat is dus niet zo, dat blijft steken rond de 20%. Het ligt niet in de lijn der verwachtingen dat dit gaat veranderen. En dat is toch raar, het is helemaal geen gecompliceerde kwetsbaarheid, waar we maar niet van af kunnen komen. Het grootste probleem daarbij is dat die bepaalde kwetsbaarheid, vooral de exploit die je daar voor kunt gebruiken die is inherent aan de programmeertalen die we gebruiken. En die talen zijn zo verschrikkelijk verweven in alles wat we draaien, daar kom je niet van af. Met andere woorden deze bugs daar heb je de komende tien jaar met precies dezelfde vorm enkel geavanceerder en in andere varianten nog last van. Zelfs zo iets primitiefs blijft de komende jaren nog bestaan.

En daarnaast heb je nog allerlei nieuwe dingen die de afgelopen jaren zijn bedacht. Met andere woorden; het aantal kwetsbaarheden (en ook de kwetsbaarheden waarvan men weet hoe deze geëxploiteerd wordt) neemt waarschijnlijk alleen maar toe. En dat lijkt redelijk fundamenteel te zijn, niet iets waar je aan kunt optrekken. Het enige wat je daar kun doen is tussen de verschillende softwarecomponenten die je hebt zoveel mogelijk “harde schotten” te plaatsen. Dus als ik jouw browser overneem, dat ik niet direct toegang krijg tot ook je database. Een aantal belangrijke principes die je daar kunt toepassen is isolatie van je software. Diginotar heeft dat slecht gedaan evenals KPN. **En daarnaast “the principle of least authority”.Alles wat je hebt, welke entiteit dan ook, of dat nu software is, menselijk kapitaal moet precies die autorisatie krijgen die nodig heeft om zijn taken uit te voeren en niet meer.** Dat betekent als er een probleem plaatsvindt, zoals een softwarecomponent dat gehackt wordt, of geheimen wil vertellen, dan kan hij alleen maar vertellen tot waar hij recht heeft. Dus alleen maar hetgeen wat hij nodig heeft voor zijn taken. Je kunt niet iemand meer privileges geven. Dat zijn wat fundamentele dingen die je daar kunt toepassen.

Verder zien we op technisch gebied dat we nieuwe ruimtes krijgen of softwarekwetsbaarheden te krijgen. Iets waar we bijvoorbeeld heel slecht in zijn is om zaken parallel te draaien, dus multicore processoren en applicaties alles draait parallel. En mensen kunnen daar heel slecht mee omgaan. De bugs die daar ontstaan zijn veel gecompliceerder vaak en veel moeilijker te reproduceren in een test situaties. Dus testen van software is alleen maar ingewikkelder geworden.

[*Refereer je hier ook aan gezien nieuwe trends op het gebied van IT zoals cloudcomputing? Men slaat bijvoorbeeld informatie op in de cloud en weet daarna niet meer waar het staat.]*. **Je kunt daar afspraken over maken met allerlei juridische redenen. Je moet weten welk recht van toepassing op de data en de service die verleend wordt. En soms weet je dat ook niet en dat betekent ook dat het een heel schemerig gebied wordt. Daarnaast spelen in de cloud ook nog meer complicerende factoren.** Wat is nou het additionele risico van dat je naar de cloud gaat en wat is nou het additionele

beveiligingsbevorderende aspect van de cloud? Ik ben er zelf nog niet helemaal uit, maar er is een aantal waardoor je kunt zeggen hierdoor zou het wel eens veiliger door kunnen worden. Je weet dat als je naar een cloudprovider toegaat met een goede reputatie dat het goed wordt beheerd. Een kleine gemeente heeft waarschijnlijk niet de expertise om al je ICT diensten die je wel moet aanbieden aan de burgers om dat goed te beheren. Als je dat in de cloud doet heb je grote kans dat een kundig persoon er zit en de zaken uit handen neemt. Dat wil in ieder geval zeggen dat je een beter beheerde applicatie hebt, maar dat betekent ook dat je een groter doelwit bent geworden. Want zodra iemand die centraal beheerde applicatie heeft aangevallen met succes heeft hij toegang tot een veel grotere hoeveelheid data waarbij de data van de gemeente er ook zit. Dus wanneer Anonymous gegevens online zet, is er grotere kans dat jouw gegevens daar na ook bij zitten. Dus dat is een additioneel risico en een beveiligingsbevorderend aspect van de cloud.

Het andere wat je ziet met de cloud is dat je niet helemaal weet wat je in de cloud moet vertrouwen. **Als je nu Coca-Cola bent met een echt bedrijfsgeheim, durf je dat aan om dat bij een ander bedrijf in de cloud te draaien. Durf je daar echt je bedrijfskritische Intellectual Property (IP) onder te brengen, waarschijnlijk niet. Dat is echt iets wat je heel goed moet overwegen, wat een risico dat met zich meebrengt.** Of dat het een corrupte werknemer van een ander bedrijf leidt. Ga je iets in India onderbrengen als het bedrijfskritisch is? Outsourcing is heel gecompliceerd. En uiteindelijk is cloudcomputing een vorm van outsourcing. Dat gaat heel ver. **Bijvoorbeeld bij outsourcing als je iets onderbrengt bij een bedrijf in India. Dan kan het zijn dat bedrijf weer een deel van zijn processen ergens anders onderbrengt. En daar kun je goede afspraken maken met de eerste hub waar je terecht komt, maar kun je dat over de gehele keten garanderen.**

[*Daar speel ik ook in met dit onderzoek. Veel bedrijven outsourcen hun IT. Ze hebben individuele verantwoordelijkheden, maar ook gedeelde. Als chain moeten ze ook samenwerken.*]. **Helemaal over de ene kant heb je geen zicht over de andere kant wat er speelt. En als er iets misgaat hoe ga je met aansprakelijkheid om?**

Ik weet niet of het iets is wat onvermijdelijk is. Je ziet dat de expertise te gering is op dit moment binnen bedrijven. En zelfs als ze het wel willen. Stel dat ze een goed informatiesysteem willen hebben in eigen beheer dat weten ze dat ze dit soort aspecten niet hebben, alleen ze kunnen niet het juiste personeel daarvoor vinden. Het is moeilijk om echt hoog gekwalificeerd personeel te vinden.

[*Bedrijven willen graag met de laatste innovaties en trends mee Ze springen op de trein mee, maar lopen qua kennis achter.*].**Kennis is echt een groot probleem. Het is niet alleen cloudcomputing. Het zijn ook andere trends en *buzz words* die een heel groot beveiligingsaspect hebben. Zoals BYOD (Bring Your Own Device). Alle bedrijven doen dat tegenwoordig, het is hip en je werknemers willen het graag. Men wil graag met eigen laptop en telefoon werken en daarnaast is het ook goedkoop. Echter, niemand weet precies hoe het exact zit met alle implicaties qua beveiliging. Men probeert dat vaak af te dichten dat je niet alles mag. Maar het is heel moeilijk om dat echt te *enforcen*.**

[*Kun je het überhaupt beveilingen?*]. Ja, dat is dus de vraag. Of kun je het veiliger maken. **Nogmaals, op langere termijn is geen enkel systeem echt veilig. Daar ontkom je niet aan, dat is fundamenteel**.

Er zijn wel zaken die je kunt doen, dus bepaalde principes terug laten keren. Zoals POLA (Principle of Least Authority) is een principe dat de hele tijd terug dient te komen. Isolatie dus "schotten" plaatsen tussen alles wat gebeurd is iets wat je altijd terug kunt laten komen. **Meer vanuit een procesmatige gedachte is security niet als een project beschouwen. Iets was je in 2012 doet en dat je project security hebt afgerond. Maar een voortdurend terugkerend proces is. En investeren in kennis, dat is heel lastig. Bij informatiebeveiliging hebben we natuurlijk dat het niet direct geld oplevert. Het is iets wat geen functionaliteit toevoegt. Dus je moet het als organisatie afwegen. De hele tijd een analyse maken is lastig. Als het mis is heb je een enorme reputatieschade wanneer al je klantgegevens op straat liggen en dat is heel naar**. Het is niet altijd duidelijk dat het de juiste investering is om het helemaal dicht te timmeren. En dat kost je verschrikkelijk veel geld wat je weer voor andere zaken kunt gebruiken.

[*Een korte recap: Vanuit organisatie is het vooral investering in kennis. En vanuit softwareorganisaties die hebben natuurlijk ook hun verantwoordelijkheden; isolation, COPA zijn de basisbegrippen voor juiste exercitie*]. **Ja, er zijn altijd antwoorden mogelijk waar in ieder geval over nagedacht kan worden maar wat niet op korte termijn gaat gebeuren bijvoorbeeld aansprakelijkheid.** Het is iets wat nu bijna nooit gebeurt, maar zodra jij een softwarepakket koopt is een van de eerste dingen die je doet alle aansprakelijkheid van je afschuiven. Je koopt iets van Microsoft, maar als er iets mis mee is waardoor je nucleaire installatie ontploft, dan is dat niet de schuld van Microsoft. Misschien is dat wel een heel verkeerd model en wat je als bedrijf dient af te dwingen. Dat is lastig, want is nooit goed aan te geven wat precies de verantwoordelijk is voor de catastrofe die in jouw bedrijf plaatsvond. Maar daar zou je wel naar kunnen kijken.

[*Het is meer richting de juridische kant van het verhaal*]. **Ja, maar de juridische kant heeft dan als bijkomend effect dat er een prikkel is om je producten beter te maken. Dus in plaats dat je geld uitgeeft. Je software wordt ongetwijfeld duurder. Want je wilt de garanties eisen en als het mis gaat dan willen we jouw verantwoordelijk stellen.** Dan zegt het bedrijf prima, dan krijg je de software drie maanden later en dan wordt het zoveel duurder enzovoort. Maar aan de andere kant geven we nu veel geld uit aan firewalls en virusscanners, zou dat geld niet beter besteedt zijn aan het oplossen van het echte probleem, namelijk dat al die software zo verschrikkelijk kwetsbaar is. Je geeft net zoveel geld uit, maar je geeft het op een betere plaatst uit.

[*Wat is de visie uw visie op de toekomst? Ik heb begrepen dat in Rusland bedrijven zijn die de hele dag aanvallen uitvoeren?*]. Ja, het is professioneel nu. Het is lastig om er een antwoord op te geven. Wat we zien is meer consolidatie. De cloud is daar een voorbeeld van. Ik denk dat je meer en meer professioneel gerunde bedrijven verantwoordelijk zijn voor je data. Maar fundamenteel heb je allerlei systemen die ICT oplossingen nu al gebruiken en daar op de toekomst als niet meer vanaf komen en die niet noodzakelijk in de cloud gehost hoeven te worden. Computersystemen die een energiecentrale draaien die gaan niet naar de cloud. Die blijven kwetsbaar en de kwetsbaarheid neemt alleen maar toe. Ik denk niet dat er meer gaat gebeuren of dat er meer moet gebeuren aan het investeren in back-up systemen. Dingen gaat nu eenmaal fout, daar houden we rekening mee en als het misgaat, kunnen we overspringen van systeem. **Als informatie is gelekt, zorg dan dat het niet bruikbaar is. Zorg dat alles versleuteld opgeslagen is. Dat zul je ook steeds meer zien**.

En wat je meer gaat zijn detectiemethoden. Niet zo zeer om de slechteriken buiten te houden. Maar er achter komen wanneer er mensen hebben ingebroken en dat je ook beter in de gaten hebt wat ze exact doen. En waar men aan heeft gezeten, wat nu lastig is. Dat was bij Diginotar en KPN het geval, het was geruime tijd onduidelijk wat er exact aan de hand was.

Wat natuurlijk ook een additioneel risico is, is dat alle systemen fysiek of virtueel verboden zijn met elkaar. Een hele hoop van de gebruikersnaam en wachtwoord combinaties in het ene systeem precies hetzelfde zijn als in het andere systeem. Men gaat niet 50 verschillende wachtwoorden hanteren, maar de moet eigenlijk wel. Dat betekent dat wanneer je het ene amateuristische systeem hebt gehackt je kunt proberen om diezelfde wachtwoorden gebruikt kunnen worden in een veel belangrijker systeem. Dus die verwevenheid van systemen gaat veel verder dan wat je in een eerste afhankelijkheidsanalyse naar boven laat komen. En afhankelijkheidsanalyse is wel iets heel belangrijks. Daar moeten we ook meer aan doen. Wat gebeurt er nou als dit domino steentje omvalt waar gaat het dan allemaal mis in de 2e, 3e, 4e, of 5e stap wellicht.

In Estland was in 2007 een aanval van Rusland op de cyber infrastructuur van Estland. Uiteindelijk leidt het omvallen van een informatiesysteem hier ertoe dat er op de straten geen melk meer te verkrijgen is. Er zitten een heleboel stapjes ertussen, maar het is wel zo. Dit soort fenomenen dat je helemaal niets met elkaar te maken hebt en dat je geen formele afhankelijkheid van elkaar hebt, blijkt dat het toch met elkaar verweven zit. **Gebruikers hier en daar maken gebruik van dezelfde authenticatie codes en dan zit er stiekem toch een op verwevenheid tussen.**

[*Gegevens wordt vaak online geplaatst en dan wordt pas actie ondernomen. Eigenlijk wanneer het te laat is*]. **Je ziet nu ook dat grote organisaties aan het kijken zijn naar methoden om in een vroegtijdig stadium te constateren dat er iets aan de hand is. Dat kan een aanval zijn, maar ook dat het systeem zich anders gedraagt dan gisteren.**

[*Dus softwarematige ondersteuning*]. **Ja, en dat is een iets andere tak van sport dan het echt beschermen van je software. Een harnas om je informatiesysteem is geweldig, maar uiteindelijk is dat harnas incompleet. Kun je detecteren wanneer is iemand binnengedrongen binnen afzienbare tijd. Dat je weet wat het geval is en niet nadat iemand pas een half jaar actief is. En dat gebeurt helaas heel vaak. De recente uitbraak van Flame welke in het nieuws is gekomen bleek dat het al jaren lang actief was, maar dat het nooit was opgevallen.**

[*En deze software had de mogelijkheid om sporen te wissen.*]. Ja, dat zie je heel vaak dat root kit-achtige capabilities voor dit type software. Je moet daar toch naar kijken, vaak wordt daar niet naar gekeken. In het geval van Flame gaat het om een bestand van 20mb. Dat ding zou je op een gegeven moment ergens moeten gaan zien. En bij Stuxnet was het een geruime tijd actief voordat het werd gedetecteerd. Stuxnet is ontdekt na een update van de makers, het zocht contact via een MSN-achtig netwerk. **Dat zijn patronen die je zou moeten kunnen herkenen. Dus als iets meer werk wordt verricht aan het detecteren van ongebruikelijke communicatie of toegangspatronen. Dat zijn ook belangrijke ontwikkelingen.**

[*Het is wordt ook steeds makkelijker tegenwoordig, standaards kits zijn beschikbaar om zelf aan de slag te gaan.*]. Ja, het is inderdaad voor het "low hanging fruit". Als je KPN wil aanvallen dat gaat je dat met die kits niet lukken. [Hetzelfde geldt voor p*hishing methodes*]. Deze methode is wel goed gelukt een tijd geleden in China bij Google en Adobe. Via deze techniek zijn ze bij de root code respository gekomen, wat ook uiteindelijk een van de redenen is waarom Google China heeft verlaten.

Het zijn wel interessante cases. Twee jaar geleden heeft de politie exact hetzelfde gedaan om een kinderpornonetwerk op te rollen. En drongen dus andermans computers binnen, wat strijdig is met de wet. Strikt genomen hebben ze bewust dat risico genomen. Het OM (Openbaar Ministerie), Lodewijk van Swieten heeft bewust het risico genomen. Het is een testcase en als we aangepakt worden gaan we dat gevecht aan. Maar dat is grappig, want ook met de bestrijding van, heb je met dezelfde problematiek te maken.

[*Vanuit de overheid schort het ook aan kennis.*]. Dat is verschillend. Je hebt team High Tech crime en die zijn echt heel goed. Zij opereren soms ook op het randje van wat mag. Het is maar een kleine club. Het grote probleem is echt een schreeuwen te kort aan mensen met kennis van zaken. De komende tijd hebben we hier ook mee te maken.

Maar het klopt als bedrijf als je naar de politie gaat dan weet de politie ook niet vaak wat te doen. En de schaal waar je mee te maken hebt is ook van invloed. Wanneer je van alles melding wilt doen dan kan de politie dat ook niet opvangen. Men werkt naar een algemene meldplicht dat alle lekken uit het bedrijfsleven verplicht gemeld moeten worden. Dat levert allerlei problemen op voor het bedrijfsleven. Zij maken zich zorgen over reputatieschade. Wie mogen de meldingen inzien. Bijvoorbeeld het NCSC (Nationaal Cyber Security Center), maar wat gaan die er dan mee doen? Je krijgt van bedrijven straks allerhande meldingen maar welke moet je wel en niet bekijken. Is er überhaupt de mankracht voor? Al dit soort dingen moet zich langzaam gaan uitkristalliseren.

Het initiatief is direct na Diginotar als wetsvoorstel ingediend. De hele 2^{e} kamer wilde gelijk alles veilig. En de motie werd aangebracht en aangenomen. En niemand had toen ter tijd het idee van alle consequenties. Het is wel ondoordacht dat dit soort zaken doorgedrukt worden. En de bedrijven zijn faliekant tegen in eerste instantie.

[*Partnering komt nu ook vaak voor. Als bedrijf je redt je het niet alleen, samenwerking is belangrijk. Zoals het delen van kennis*]. **Heel veel wordt al gedaan op informele onderonsjes. Zoals de banken hebben om de haverklap onderonsjes. Die willen dat niet in de krant hebben. Maar die hebben onderonsjes ook met NVB (Nederlandse Vereniging van Banken) en op dat moment wordt informatie uitgewisseld. Dit is iets wat in grote bedrijfstakken speelt. En de vraag is nu of dit anders gaat worden met een wet en publieke meldplicht. Het wordt dan een spel van advocaten. Wat kunnen we melden zonder dat we teveel prijsgeven. Partnering zie je dus. Bedrijven hebben er interesse voor, maar zijn nog huiverig. Zodra het formeel wordt, wordt het lastig.**

[*Ook op nationaal niveau wapent Nederland zicht voor aanvallen op digitaal vlak*]. Ja, onderzoeksprogramma's worden opgestart waarbij ook pro actieve cyber security inzit. En Nederland

maakt zich zorgen. De aanval op Iran is de aanval van een natie staat geweest. Er werd altijd een beetje lacherig over gedaan, maar we hebben nu de eerste case gezien van een aanval op een land.

Expert 2

[*Introductie model*]. **In plaats van opmerkingen over het model te geven wil ik eerst starten met een aantal vragen. Het model (cyber governance model Betz) kende ik nog niet. Ik ben heel erg van de school PPT (People Processes Technology). Mijn eerste kanttekening was inderdaad ik mis in het middelste van cyber mis ik 'people'.** [*People is inderdaad niet gemodelleerd in het model, echter is zo verweven met de pilaren processes, information en technology dat people niet expliciet wordt vernoemd.*]. **Information in het model noem ik liever assets, echter dan wordt het nog verwarrender.** Maar laten we het model van Betz niet ter discussie stellen, dat leidt alleen maar af. Bij dezen is dat gezegd.

Het tweede is ook één van de hamvragen. In je model heb je het eigenlijk over operationeel/tactisch en strategisch als ik het heel plat sla. Ik denk zelf dat, maar dat is een persoonlijke mening, dat het operationeel/tactische stuk in het model […]. **Hoe je het ook went of keert, en dat merk ik ook bij NSCS discussies, heel erg drijft wat er strategisch gebeurt. In tegenstelling tot, ik noem het maar even de "maakbare wereld" waar dit soort loops vaak op strategisch niveau gebaseerd zijn. Geloof ik op dit moment, met nadruk op dit moment niet in die maakbare wereld. Dus wellicht teken je het per ongeluk of expres goed die pijl hier, maar ik denk dat het effect groter is op operationeel tactisch niveau, dan op strategisch niveau.** En, nogmaals dit is niet zoals je het zou willen als mens of als business manager, maar het is wel de praktijk. En dat komt voor een deel omdat het (wederom persoonlijke mening, maar dat laat ik vanaf nu achterwege) waar het daarstraks al over hadden, het gaat over alles en niks. Integraal en je kunt zelfs zeggen is hier vanuit cyber perspectief een aparte initiële loop (of hoe je het ook wilt noemen) voor te definiëren. Een voorbeeld; het KLPD (Korps Landelijke Politiediensten), de politieacademie, neigen op dit moment heel snel naar: *we praten niet meer over cybersecurity*. Wij praten over misdaad, vanuit hun perspectief gezien. Misdaad met IT middelen. Voor het KLPD is cybersecurity niet anders. Waarom? Wat je zelf ook als schrijft; de mens speelt een heel belangrijke rol, APT's (Advanced Persistence Threats), die je ook al beschreven hebt. Daar zit eigenlijk, wanneer je het plaat slaat, relatief steeds kleinere componenten aan cyber in. De vraag is even of dit heel anders wordt dan de normale governance voor je bedrijf. En of je het wel af kunt splitsen van je bedrijf of van je overheidsinstelling of als regering.

[*De bedoeling van dit model is inderdaad de implementatie van het model binnen het reguliere ERG (Enterprise Risk Governance)*]. Inderdaad, dat heb je ook beschreven. Dit waren dus de eerste twee dingen die mij naar binnen schoten. **Dus operatie en tactiek drijven strategie op dit moment. En dat heeft vooral met het enorme tempo te maken. Op operationeel niveau zijn de ontwikkelingen ontzettend kort cyclisch. En dan praten we over minuten soms. Terwijl met de strategisch slagen is men gewend om in maanden of jaren te praten. Ook een effect zal zijn dat deze cyclus voor mensen die dat niet gewend zijn, dat merk ik echt in de praktijk op het management, die zal veel sneller moeten dan ze gewend zijn.** Ik deel bijvoorbeeld mijn werkruimte, veel overleg en resources met mijn quality collega. En dan meer ik gewoon dat die cyclus binnen quality management vele male trager, meer doordacht (en dat bedoel ik niet flauw), bedachtzamer is dan dat we bij security gewend zijn.

[*Ik heb het idee dat het nog vele brandjes blussen is*]. Ja voor een deel wel. Aan de andere kant ben ik weel een optimist anders had ik het al opgegeven. We worden wel steeds slimmer. Alleen is het wel en dat zie je ook in het laatste cyber security beeld, want internationaal wordt het ons ook flink ingewreven. **De andere kant wordt steeds slimmer. Er zijn steeds meer resources aan de andere kant, zowel financieel. En dat is ook een punt, deze partijen hebben steeds meer te maken met langere ketens. En je hebt dat ook aangegeven in je onderzoek. Er zijn steeds meer partijen betrokken, alles hangt aan alles samen. En dat maakt a, dat de slagkracht veel minder wordt. Maar b en daar heb ik echt dagelijks last van, dat het steeds moeilijker is om verantwoordelijkheden te benoemen.** En dat mensen steeds verder afstaan van de kwetsbaarden of de feitelijke dienst. En dat voornamelijk geldstromen dusdanig complex zijn, weer afhankelijk van diezelfde verantwoordelijkheden. En dat niemand eigenlijk zegt we hebben die funding nodig. We hebben die discussie ook met het NCSC. Op dit moment zie je en dat is positief, dat de overheid zegt, de enige manier waarop mensen het gaan doen is wet en regelgeving afdwingen. Het is heel simpel in ons vak is het zo als u vraagt wij draaien als u maar betaalt, heel plat gezegd. **Dan blijkt het voor opdrachtgevers, omdat zij ook maar een klein deeltje van de keten zijn, van producent tot eindafnemer, dat zij ook op gebied van cyber en management security aspecten, dat het toch verder voor of achter in de keten moet, maar zeker niet bij ons. De enige respons die als gezond verstand ontbreekt, is dat wet en regelgeving dat maar moet gaan oplossen.** Aan de andere kant zie je dan weer de mismatch tussen de traagheid zoals de AOW (Algemene Ouderdoms Wet), van wet en regelgeving het stuurmechanisme wat daar op zit. En dat zijn alle delen die jij hier zet (operationeel) en wat hier eigenlijk feitelijk allemaal aan het gebeuren is.

[*Is het zo dat organisaties zelf ook actief zijn, in het bijzonder op het gebied van verantwoordelijkheden? Ook omdat men vaak te maken heeft met derden?*]. Wat je ziet, maar dat is dan typisch even in onze sector management services providers. En dat is dan weer een andere tak van sport omdat wij met heel veel partijen zaken doen. Wij proberen dat in één infrastructuur, shared services of processen samen te laten komen of business cases. Business cases is dan geld en kennis. Wat je ziet is dat vanuit compliance perspectief worden er steeds hogere eisen aan ons gesteld, generiek. En omdat wij shared service leveren is het generieke prima. Alleen waarin het beter kan is dat, wij doen met heel veel verschillende sectoren zaken. Dat varieert van overheid tot bedrijven. En ergens komt dat allemaal samen in het zelfde operationeel tactische framework en waar wij die klanten mee bedienen. En waar op basis van contractafspraken worden gemaakt. En dan zie je vaak weer, dat de klant, zeker onder druk van wet en regelgeving (denk aan overheidsklanten) extra eisen stellen. Dan wordt het voor ons moeilijker, niet onmogelijk. En dat het voor ons duurder en moeilijker wordt om operationeel op te reageren omdat je met specifieke mensen moet gaan werken. Gescreende mensen, specifieke infrastructuur, het woord de cloud of BYOD (Bring Your Own Device) zal ik maar niet laten vallen, maar dat trekt een blik open dat wil je niet weten. **Het is steeds lastiger ook al omdat we één van de blokjes zijn in die hele lange keten van een provider. Het overzicht van die ketens en de architectuur en daar wil ik naartoe, van die ketens, zowel technisch als qua processen, maar ook qua contractsamenstelling is zo waanzinnig complex tegenwoordig. Dat is echt managen.** Ik ben te ver van de vraag afgedwaald.

[*Het is interessant, want het is ook de kern van het probleem*]. Ja, het matcht met het integrale verhaal. A, het gaat over van alles en nog wat qua onderwerpen. Type bedreigingen, doel van de bedreigingen en het verschil wat je hebt beschreven. **En als je dat koppelt aan de complexiteit van**

de delivery ketens (noem ik maar eventjes), dan kom je eigenlijk als je het zou tekenen op een heleboel van dit soort plaatjes terecht en dan nog in drie dimensies. En op de één of andere manier zou je daar inzicht in moeten krijgen en dan kom je op het op toverwoord. In al val dit soort zaken zou je in architectuur moeten denken. Dus zowel de techniek, security by design. Daar praten we nu al heel technisch over met klanten. **De zaken gaan echter wel veel sneller dan dat er op gereageerd wordt. Inmiddels is de strategische loop zover om over security bij design te gaan denken. Laten we daar ons regelmechanisme op loslaten. Maar dat is heel erg op techniek gericht terwijl we inmiddels al op de fase zitten van APT's, BYOD, social media. We zijn daar al lang mee bezig maar op strategisch niveau is daar nog volstrekt niet over nagedacht. De technische architecturen dat gaat best goed, maar inmiddels zouden we daar toch verder in moeten zijn. Want de architectuur gaat ook over mensen, processen, informatie en dat is vele malen moeilijker.**

[*Inderdaad, in navolging heb ik wel een ideaal beeld geconstrueerd*]. **Ja, dat klopt, maar je model geeft wel de gewenste situatie weer. En dat je qua maturity nog niet zo ver bent… En dat operationeel razend snel draaien, tactisch redelijk snel, maar die zijn al aan het laggen als je het vliegwiel erachter denkt. En strategisch laat volstrekt na. Dat zie je ook bij degene die besluiten moeten nemen. Dit werkt alleen als er voldoende funding is en als mensen gedreven zijn om het te doen.**

[*En dit tracht ik aan te geven met de resources zoals deze gepositioneerd zijn in het framework*]. **Inderdaad, op dit moment is het de gedrevenheid van mensen die zorgt dat we het als maatschappij nog redelijk doen. Dat we nog redelijk op onze burgers en klanten letten. Dat is op dit moment een grotere factor dan het feit dat deze kring (strategisch) voor de juiste aandacht, de funding, de juiste wet en regelgeving. Deze helt echt na op dit moment. We hebben een governance probleem. En dan ga je heel erg drijven op de vakmatige passie van mensen. En het gezonde verstand van mensen die op tactisch niveau knopen doorhakken.**

[*Het gezonde verstand en awareness waar ik toch de nadruk op leg in het onderzoek. Hoe creëer je awareness bij mensen. Mensen moeten eerst tegen de muur aanlopen alvorens ze wakker worden.*]. Ja, dat is agendapunt 1 bij mij. Mensen die op operationeel niveau werken ben ik hoopvol. Daar gaat men de juiste dingen roepen. Dat is echter bij ons bedrijf, dus wellicht een beetje vertekenend. Waar ze alleen last van hebben is dat ze soms in hun schulp moeten kruipen. Mensen die veel verstand hebben van hun vak maar het slecht kunnen uitleggen aan andere mensen. En dat er een kloof aan het ontstaan is in hun omgeving en pas wakker worden als het kwaad geschied is. Dat is ook overigens de awareness tactiek die ik al een jaar handhaaf. **Ik heb heel veel aandacht met de mensen op het gebied van Seurity Incident Reporting enerzijds doe ik dat vanuit een monitoring en repsons perspectief, maar elke case heb ik zeer hard nodig. Vooral om mensen op tactisch en strategisch niveau duidelijk te maken dat dit echt aan het gebeuren is.**

[*Het wordt het door organisaties ook gezien als een last. Men moet voldoende resources ter beschikking stellen, als tijd en geld.*]. **Dan bestaat de organisatie uit twee delen. De mensen die wat willen verkopen willen dat zo goedkoop mogelijk doen. En er zijn mensen die er geld aan kunnen verdienen. Dus tegenstrijdigheden binnen een organisatie. En die probeer ik in mijn rol ook te verenigen. Dit (het framework) is nog steeds vanuit de consultant gezien de maakbare wereld. En**

ik geloof persoonlijk niet in deze maakbare wereld. Maar de op operationeel niveau zie je dat mensen het beginnen te snappen.

[*Vooral ook zorgen dat security binnen het management komt*]. Ja de juiste aandacht. En dat is voor mij het moeilijkste van het idee afbrengen dat ze in een maakbare wereld leven en een begrensde wereld. Qua infrastructuur zijn er geen grenzen. Mensen kennen geen grenzen. Maar dit is wellicht vervelend voor je onderzoek. **Cyber is als het goed is ook in de politiek. Over een paar jaar praten we er niet meer over. Maar jouw lijstje van cyberdomeinen heeft voor mij wat voor opgeleverd wat we op dit moment op het gebied van cyber verstaan.**

[*Het model zoals het hier staat op basis van literatuur, praktijk etc Zijn er concepten die missen. Is er wat opgevallen.*]. **Wat ik voornamelijk dit blok (reputation & assets) miste of niet snap. In feite gaat hier platgeslagen om gewin en om continuïteit. Reputatie is belangrijk, maar voor mij is dat niet meer dan een asset. Ik kan hier wat makkelijker denken in de termen van continuïteit.**

[*Klopt, gekozen is ook meer vanuit een eenvoudig oogpunt om het gemakkelijk te maken, vier r-en die pivoteren rond cyber*]. Ook belangrijk, een boodschap die komt maar niet land heeft ook geen zin. En assets is wat mij betreft continuïteit en dat is ook wat je hebt uitgeschreven. **Het profiel van aanvallers, ze hebben een verschillend doel. Alleen dat zie ik minder terug. De risks lijst is vrij uitgebreid. Ik zocht nog wel naar de aansluiting met de impact van de specifieke risks. Met wat je net zei; ik snap de woordkeuze. Maar dat was er wel één waar ik op bleef hangen.**

Als je het hebt over deze loop (strategie) en je zou prioriteiten willen stellen. Als ik het model zelf zou tekenen, dan zou ik deze meer hiernaartoe schuiven (tussen risks en reputation). Want dit is nog een beetje het maakbare stuk. Maargoed dat is ook weer een kwestie van tekenen. Het maakt niet het model verkeerd.

Als je het over de praktische bruikbaarheid van het model zou moeten hebben, dan kun je deze zeker gebruiken om het uit te leggen aan het management. Maar dan zou ik de loop verplaatsen (operationeel). Dit is een zodanig beweeglijk verhaal, verspil hier niet teveel energie op. **En dan terugkomend op awareness wat je ziet is dat mensen zichzelf al sneller corrigeren. In het response gedeelte worden mensen toch veel slimmer.** [vertrouwelijk voorbeeld]. **Het slechte nieuws is wel dat deze groep (strategische gedeelte) het minder snapt. Het gaat te snel.**

[*Terug naar de praktische haalbaarheid van het model. Hoe zou een dergelijk model in de praktijk ingezet kunnen worden? Zodoende dat een manager er mee aan de slag zou kunnen gaan. Ofwel de praktische toepasbaarheid van het model*]. Wat het mooiste zou kunnen zijn is dat en dat geldt voor elk model wat je introduceert is kijken naar best practices. Dus uitproberen hoe dingen werken. Het nadeel is dat op een dergelijke manier het gaat leiden to certificeringvragen en processen en dat mensen ermee op de loop gaan. En voor dit onderwerp is het een risico. Het zou heel pragmatisch, dynamisch en volatiel moeten zijn. Maar het probleem met dit model is dat het nog veel te snel gaat (operationeel). Qua tempo heb je het goed weergegeven. Eigenlijk zou je er nog één bij moeten tekenen op tactisch niveau. En dan de vraag is of je het overdrachtelijk wil maken, waar zit de

aandrijving? [*initiële visie is vanaf strategie*]. Mijn visie is dat de aandrijving op operationeel niveau gebeurt.

Terugkomend op de praktische toepasbaarheid, ik denk dat je daar rekening mee moet houden. Daarnaast zou ik het graag zien gekoppeld aan “architectuur denken”.Dus niet enkel de techniek, maar de samenhang tussen techniek, processen etc.

En ik ben een heel sterke gelover van een checklist benadering. Dus beschrijf niet alles in detail, maar een repository van alle checks die je als bedrijf moet afvinken als bedrijf. Als je het over awareness hebt, daar zijn vele checklists voor. Maar als je het over assess hebt dan kun je een checklist maken van best practices. Dit zijn de onderwerpen waar je dan als bedrijf over nagedacht moet hebben. Op het gebied van architectuur, je awareness in je monitoring etc. En dat geldt dan ook voor detect, partnering etc.

Vanuit mijn hobby vliegen heb ik veel waardering voor wat we hebben bereikt. Daar zijn checklists niet buiten te denken. Maar die wereld is vergelijkbaar met de IT wereld. En wellicht is de luchtvaart nog complexer, daar zijn ook vele variabelen. Mensen maken bijvoorbeeld fouten, dat gebeurt. En dat is niet maakbaar, maar opgelost met vrij strakke regels. En in het ontwerp zijn al die niet maakbare omstandigheden in meegenomen.

[*Compliance is in dezen ook heel belangrijk*]. Ja, dat klopt. [vertrouwelijk voorbeeld] Ik ben wat cynisch over het feit hoe we als bedrijven en overheid omgaan met compliance. Ik geloof dat het nog steeds nodig is om een aantal basale dingen op te schrijven. Maar het is steeds moeilijker om alles op te schrijven en af te dichten. **Ik geloof toch steeds meer in het zelf corrigerende mechanisme wat hier zit (approach in het framework). Daarvoor is het nodig dat mensen met awareness de risico’s snappen en weten waar het inhoudelijk om gaat. En daar helpt elke checklist, gekoppeld aan een regel loop bij.**

Het model nogmaals, is denk ik heel erg bruikbaar. Ik denk dat deze (tandwieltjes) gelet op de discussie wel aardig is dat er een derde bijkomt. Inclusief het aandrijfverhaal, welke as bepaalt nu de frictie. Als je het hebt over dit model dan snap ik het en dan kan ik het ook gebruiken, mits daar best practices achter komen checklist/repository achtige constructies.

Resources had ik overig wat meer moeite mee. Uiteindelijk zijn alle resources gebaseerd op funding. Wellicht ben ik hier teveel beïnvloed door mijn eigen sector. Dus platgeslagen heb ik eigenlijk altijd maar twee resources nodig. De passie van mensen in hun vak of hun agenda. Het tweede is het concrete funding, geld. Ik snap hoe de zaken zijn gepositioneerd maar ik zou toch nog op de één of andere manier het aspect geld meer terug laten komen. Bijvoorbeeld in met een business case en deze er hard tegenover zetten. Omdat ik dan de resources en de reputation direct met elkaar in verband kan brengen. Dan krijg je meer balans en kan men ook de keuze maken van ik doe het wel of niet. Dus naast human en organizational resources zou ik heel erg het aspect funding en geld sterk benadrukken. Want dat is de meest harde vorm waar de loop door wordt beïnvloed. Je kunt het ook zien als stroomkanaaltjes. Als je resources heel dun zijn zul je zien dat het de wrijving van de loop beïnvloed en dat het invloed heeft op de response.

[*Uiteindelijk staat aan beide kanten van het spectrum geld gepositioneerd*]. **Ja klopt. En dat sluit mooi aan bij je risk benadering die je terecht zegt. Dit is puur in feite de risicoanalyse (risk) in combinatie met de andere zaken die je er op loslaat.** En hier (response) gaat het er echt om van doe ik er wat aan, of doe ik er niks aan. We accepteren ook heel veel risico's met elkaar als maatschappij en bedrijf. Zoals internetbankieren op de mobiele telefoon.

Wat ik wel miste vooral in je verhaal was het woord vertrouwen. Maar dat heeft weer sterk te maken met het feit dat ik vooral deze loop (strategisch) probeer te beïnvloeden. Zowel aan de vraag als aan de mitigerende kant is vertrouwen het toverwoord. Je gebruikt iets omdat je vertrouwen hebt. Is er een incident dan wordt dat in de operationele loop direct gecorrigeerd. Dan heeft het bedrijf reputatieschade en dan worden de resources aangesproken, maar het correctiemechanisme werkt wel.

[*Is vertrouwen te scharen onder reputatie?*] Ja, maar dan maak je het niet gemakkelijk. Vertrouwen is toch gebaseerd op de slimme dingen die mensen hier (respons) doen. Dat heeft ook te maken dat men hier risico's neemt in het vertrouwen dat een ander zijn werk wel goed doet. Het moment dat het vertrouwen geschaad wordt dan heb je hier een reputatie probleem (reputation). Maar in feite komt reputatie in al deze aspecten terug. **Met risks praat je in feite over wantrouwen en hier praat je in het vertrouwen (approach) dat het juiste gebeurt. Ja, reputatie speelt een rol, maar het heeft ook te maken met dat anderen ook slim acteren.**

Als je kijkt naar de Olympische Spelen waar wij ook een rol is spelen, dan zijn de contracten heel simpel. Veel partners werken samen. De onderlinge contractstructuur is erg dun. Ze hebben ook allemaal één doel en dat is dat de reputatie niet beschadigd wordt. En in hun regelmodel ligt dus bijna geen compliance verhaal achter. Bijna niemand kan zich beroepen op de contracten onder "jij zou dit doen". Het wonderlijke is dat het werkt. Er ligt een afspraak met het IOC dat wanneer partijen toch niet overeen komen het IOC kan benaderd worden. En dat is nog niet gebeurd. Men streeft naar één doel. Men kijkt niet meer naar compliance maar gewoon kijken naar effectief managen van deze kringen.

[*Zijn er ook gezamenlijk verantwoordelijkheden?*] Bijna niet. Zoals het daar werkt en het vertrouwen onderling is bijzonder. Op kleinere schaal zie je het ook gebeuren. **Vier jaar geleden zou het ondenkbaar zijn dat ik met collega's van andere bedrijven rond de tafel zit om over cyber security te praten. Onder druk van wat we meemaken is dat aan het gebeuren. We delen informatie met elkaar, wel onder zware restricties. Maar vertrouwen wat nodig is voor het regelmechanisme begint op gang te komen. Zo is er ook een van het transport en de financiële sector. Omdat de dreiging zo groot is van buitenaf in gesprek zijn. We hebben allemaal onze eigen belangen maar het is van groot belang dat de maatschappij vertrouwen blijft houden in de financiële sector en logistiek. Dit is allemaal gebaseerd op een vertrouwensloop. Vertrouwen in elkaars vakkennis en delen van informatie.**

Expert 3

[*Introductie model*]. **Als ik kijk naar dit model dan vind ik het redelijk compleet. In cyber heb je de drie pilaren benoemd. Eigenlijk zou je technology ook nog kunnen uitsplitsen in architecture en**

technology. De technologie zelf en de architectuur die daar op gebaseerd is. Dus dat is één blok welke je wellicht nog kan benoemen. Voor de rest denk ik wat er nu in zit redelijk compleet is. Het draaien van de tandwielen vind ik ook goed bedacht, dat de strategisch loop sneller draait dan de operationele. Soms heb je twee à drie cycli nodig om een goede sturing the kunnen initiëren.

[*Wellicht zou er dan nog een tandwiel tussen moeten om operationeel, tactisch en strategisch te waarborgen zodoende de strategische loop langzamer in de pas te laten lopen. En dan is de vervolgvraag, wat stuurt wat aan? In eigen visie is dat de strategie welke zich door de organisatie heen nestelt*]. **Wat wij zelf zien is dat wij strategische plannen opstellen en die plannen strekken zich meestal uit van drie tot vijf jaar. Een strategisch plan voor technology risk dan kijk je drie, vier jaar verder. Maar toch heb je ieder jaar een meetmoment. Het kan best zo zijn dat een strategisch plan van drie, vier jaar aangepast moet worden ten aanzien van het deel wat je gemeten heb op tactisch niveau van afgelopen jaar.** Als je kijkt naar de maatregelen die je genomen hebt om groei te realiseren effect hebben gehad, je kijkt altijd even terug. In dan opzicht zou een extra tandwiel in het model beter uitleggen wat je moet aanpakken.

[*Eigenlijk is in het operationeel model ook de tactische laag verwerkt*]. J**a, wat je ook ziet is als je kijkt naar deze tandwielen dan is het voor technologie ook anders dan voor processen. Als je kijkt naar processen heel vaak blijven deze langer intact. Maar de technologie gaat zo snel, dan moet je weer vaker bijsturen. Dus afhankelijk van welk deelgebied je zit zul je misschien vaker of minder vaak moeten bijsturen. Dus dit wieltje wordt afhankelijk van in welk deel je zit groter of kleiner. Het verschil tussen het tactische en strategische wiel is naar mate je op technologie of proces zit kan variëren. Misschien dat je daar nog wat over kan zeggen.**

Je ziet dat bijvoorbeeld ook in een samenwerkingsverband. Een paar maanden geleden zijn we een samenwerkingsverband aangegaan met een projectgroep in Eindhoven (TU Eindhoven), die zijn een bedrijf opgestart (Salescope). En dat is eigenlijk als een half jaar, jaar bezig met het ontwikkelen van cyberaanvallen in een vroegtijdig stadium, die hebben daar een tool voor bedacht. En dan stond er recentelijk in het nieuws dat de Universiteit van Amsterdam bezig is met ontwikkelen van een tool om cyberaanvallen in een vroegtijdig stadium inzichtelijk te maken. En als ik dat vergelijk met wat ze in Eindhoven doen dan is dat identiek enkel met een andere aanpak of variant om dat visueel te maken. Je ziet dat de visuele ontwikkeling die ze in Eindhoven gemaakt hadden significante verschillen toonden met het werk in Amsterdam. Dan zie je dat in driekwart jaar je de verschillen in de technologie terugziet en in het bedrijfsleven. Heel vaak zie je al bij defensie die in voorstadia dat soort dingen ontwikkelen om cyberaanvallen zeg maar in een vroeg stadium op te pakken. [*De ontwikkelingen gaan heel snel*]. **Inderdaad en dan zie je dat het operationele wiel voor technologie heel groot is, het tactische niveau kleiner en het strategische niveau nog kleiner. Dus eigenlijk kun je voor technologie niet verder dan drie jaar kijken. Terwijl je voor processen best vijf jaar verder kan kijken. En dit is wellicht ook goed om te benoemen in het onderzoek.** Als ik naar je rapport kijk dan kan dit wellicht in je conclusie terugkomen. Verder ziet het er goed uit.

[*Met dit model schep ik een ideaal wereld. Mijn idee is dat de strategie de operatie aanstuurt. Wat is hier de visie op? Uit recentelijk onderzoek naar gemeentes en IT veiligheid dat dit nog niet was doorgedrongen op strategisch niveau.*]. **In principe zie ik dat ook. Bij [gefingeerd] zie ik bijvoorbeeld**

dat de CISO (Chief Information Security Officer) rapporteert aan de financieel directeur. En niet direct aan de CEO en dat is heel vreemd. Blijkbaar heeft de CEO minder zicht op de CISO en kan hij daar minder op sturen, dit in tegenstelling tot je model van wat eigenlijk de bedoeling zou moeten zijn. Maar op management niveau helt het toch een paar maanden na voordat het binnendringt.

Je ziet bijvoorbeeld ook dat er heel vaak producten worden verkocht en die hebben ook een security aspect. En dat wordt mee verkocht aan de klant, maar wanneer de klant er om vraagt blijkt het er toch niet te zijn. **En dan zie je inderdaad dat de operationele aspecten sturing geven op strategisch niveau. Dus je ziet inderdaad in de praktijk dat het is omgekeerd en dat de operationele aspecten de strategie bepalen.**

[*Zou het wenselijk zijn om aansturing beginnende vanuit de strategie te voeren?*]. **Dat is inderdaad wenselijk, echter in de praktijk gebeurt het niet. Het management is vaak niet op de hoogte van de echte dreiging. En wat de impact is van de dreiging alsmede van de kwetsbaarheden. Waar er eigenlijk naar mijn mening behoefte aan is om de risks uit het model veel visueler te maken voor managementlagen.**

[*Hoe creëren we awareness met een dergelijk model. Ik heb het idee dat men eerst tegen de muur aan moet lopen alvorens er wat gebeurt.*]. Bij het bedrijf waar ik nu zit maken we gebruik van een partij welke informatieve filmpjes ontwikkeld op het gebied van security. Er worden dan actuele filmpjes naar de medewerkers getoond waar het management ook achter staat. En daar zitten ook heel specifiek awareness filmpjes bij. Op die manier maken we een awareness programma heel specifiek voor de branche.

[*Hoe kan dit model nu praktisch worden ingezet? In dit onderzoek gaat het om sturing vanuit de managementlagen.*] Wellicht zou je er op operationeel niveau nog wat aan kunnen sleutelen om het inzichtelijk te maken voor de managers. En dat je dan ook aangeeft wat de specifieke uitgangspunten per blok zijn. Wat bedoel je er precies mee.

[*In het onderzoek is dit reeds verwerkt, wellicht wat vlak. De bedoeling is ook om met dit onderzoek managers handvatten te geven met een model wat generaliseerbaar is voor meerdere organisaties; een high level overview. De vraag is of het dan compleet genoeg is en of dat bepaalde concepten meer toelichting geven.*]. **Het is natuurlijk wel zo dat awareness al een heel programma is en dat daar veel meer bij komt kijken, zoals psychologische aspecten. Dus hoe reageren mensen op bepaalde aspecten. Door awareness heb je minder incidenten. Of juist meer omdat mensen het meer gaan melden. Daardoor krijg je meer sturing of kun je beter sturen als manager. Dieper uitwerken van het concept awareness zou passen in een andere studie.**

[Voorbeeld van BYOD met het beheer van privé en zakelijke gegevens op de smartphone. Het is lastig om apparaten van derden te beheren. Het voorbeeld toont een applicatie welke de data encrypt en het mogelijk maakt het apparaat op afstand aan te sturen, zowel door de manager uit de organisatie als zelf.]

[Een model is getoond op basis van verschillende threat agents. Dit zou in de revisie van het model meegenomen kunnen worden.]

Expert 4 (telefonisch)

[*Introductie model*] **Met betrekking tot approach komt het wat onduidelijk over. Ik lees approach als meer als een theoretische approach. Ik doe een assessment, kijk naar verschillende scenario's en op basis van deze informatie maak je een response plan. Dat zou ik verstaan achter een approach. Maar echt de activiteiten, de operational activiteiten die mis ik hier.**

In het governancemodel heb je het over verschillende procesinstructies. Wanneer we spreken van een incident en we kijken naar de approach. Wat zegt een bedrijf dan, we hebben onze controls niet goed geregeld en daarom is het incident ontstaan? Of is er iets mis met de policy waardoor het incident is ontstaan? Of er moet een aanpassing gedaan worden op de controls of op de policy. En in het proces zou dat ook nog ergens moeten terugkomen.

[*En dat is op tactisch niveau, of is het ook op operationeel niveau?*]. Dat hangt er vanaf. Als er een instructie niet goed is beschreven dan is dat operationeel. En bij een policy is dat hoger en dat heeft invloed op het governance model.

Dan kijkend naar resources (human/organizational) en deze die gebruik je als basis voor de response. Deze moet je wellicht nog wat meer verduidelijken. De resources zoals ze nu in het model zijn gedefinieerd, zijn wellicht nog niet duidelijk genoeg en vooral ook in relatie met de uitwerkingen. Daarnaast is het wenselijk om ook te kijken naar reputation en assets en deze verder uit te werken.

[*Praktische toepasbaarheid*]. Je zou het framework verder moeten uitbreiden zodat het voor organisatie gemakkelijker wordt om het in te zetten. En daarnaast om de praktische toepasbaarheid te vergroten is wellicht een gap analyse binnen een bedrijf wenselijk om de inzetbaarheid en toepasbaarheid van het model te vergroten.

Expert 5 & 6

[*Introductie model*]. Noem mij eens een proces. [*Ik zie het als een logische laag. Denk aan de loginprocedure van mijn smartphone op het bedrijfsnetwerk (BYOD)*]. Dus het proces is inloggen. Waarom log je in? [A*uthenticatie*] Inloggen is een onvoorwaardelijk proces om te komen in een hoofdproces. Je logt ergens op in om iets te doen. We nemen Bol.com als voorbeeld. Dan is het proces waarvoor je inlogt iets om te bestellen of bijvoorbeeld om een bestelling na te kijken. Als dat je proces is, dan ben ik hier een beetje mee aan het stoeien (cyber). **Als ik het model interpreteer, na het onderzoek gelezen hebbende, dan is cyber twee typen processen. Je hebt processen om je primaire proces uit te voeren. Zoals boeken bestellen bij Bol.com. Daarvoor heb je informatie nodig, welke komt van de leveranciers van die boeken. En dan gaat de gebruiker bestellen en betalen, welke processen zijn. Net als dat iDeal bij betalingen een subproces is. Daarvoor heb je technologie nodig, het moet veilig en dan gaat de informatie over en weer. En dat is een beetje hoe de processtructuur werkt.** Waar ik nu moeite mee heb is dat als je het model zo positioneert, kan ik ook zeggen dat zie je verkeerd want het is een hoger niveau. Dit is er op gericht om je primaire

processen te beschermen. **Dit zijn niet de primaire processen, dit is cyber defense, intrusion detection etc. Daarvoor heb ik nodig informatie vanuit het primaire proces en daarvoor gebruik ik een firewall en die en die. Die laatste is logischer. Want dan klopt je governance, dan zijn dit de uitvoeren processen van de governance structuur omdat je deze koppelt aan het piramide model in je onderzoek dat is wat bescherm ik.** Je beschermt je primaire proces, daarvan zeggen wij dat kan niet, want dat is te complex. Dus richt je noodzakelijk om de belangrijke informatie in dat proces en haal daar de benodigde technologie bij en die ga je beschermen. Dus je assessment detection etc, draait om cyber om deze te beschermen. **En dat loopt een beetje door elkaar heen. Je hebt twee typen processen cyber processen, de cyber beschermen van je organisatie. En je primaire processen, ofwel waar een organisatie uit bestaat en deze twee lopen door elkaar heen.**

Dan wordt deze (operationele loop lastig), want ik heb hier mee zitten stoeien. Want als je het als primair proces definieert dan kom je namelijk niet uit, dan krijg je een uivorm. Dan heb je een meerlaags model wat steeds groter wordt. Dat begint met technologie, daarin zit informatie, daar zit een proces omheen, een ecosysteem, partners, dan krijg je een gelaagd model. En in die zin is dat logisch want dan krijg je er allemaal lagen omheen zodat je proces beschermd blijft. Daar zit ik dus een beetje mee. Is dit een cyber operations model? In het drie staps model wat ik je heb gestuurd zit de OEDA (Observe, Orient, Decide & Act) loop. Dat is een typische defensie term maar die zie je ook steeds meer bij cyber defence ontstaan. Dat komt ongeveer hier mee overeen (response). **Waar ik dan een beetje moeite mee heb en het er ook tussen vind zweven is de responsibility in vergelijking met het OEDA model. Responsibility en partnering zijn niet gelijkwaardig qua niveau.**

[*Die zijn bedoeld voor het eigen software ecosysteem. Samenwerking tussen meerdere partijen, vandaar ook in de response sectie. Een projectaanpak kan niet zonder de juiste verantwoordelijkheden*]. **Nee, maar hij zit, en dan kom ik bij een punt wat ik hier had (strategische loop). Ik zou deze andersom verwachten. Hier zit de analyse, wat moet ik beschermen en hoe ziet dat er uit. En dan komt de assessment, als ik weet wat ik moet doen, wat moet ik dan doen? Dat is de assessment welke spelers heb ik, dat is de assessment welke processen dus dat zit allemaal in die hoek. Uit die assessment komt eerst je governance. Dit is mijn ecosysteem, dit zijn mijn partners en daar de organisatieonderdelen die als kritiek bestempeld zijn. Hier moet ik mijn governance uitoefenen. En als ik mijn governance niet kan uitvoeren dan moet ik gaan partneren. Als jij defensie bent en je wil jezelf veilig stellen dan komt de vraag mag ik draaien op Windows? Je bent niet de eigenaar van de software. Dus governance technisch kun je dat willen en vanuit hier ook noodzakelijk vinden. Maar draai je op Windows, dan moet je vanuit governance gezien een duo governance aangaan.** Ik heb mijn governance, maar Microsoft, mijn leverancier heeft zijn eigen governance. En dan krijg je eisen zoals Microsoft is ingericht, security organization, quick response force. Dat is de governance aan hun kant en dan krijg je een extra strategisch hulpwiel, zelfde tools, zelfde instrumenten. Maar om dat hele ecosysteem dicht te zetten heb je er al twee. Pas als je weet hoe dat er uit ziet kun je een coach opbouwen, want dat betekend ik heb een interne coach. Daar ben ik verantwoordelijk voor, dat is mijn domein. Maar mocht het buiten mijn domein liggen, dan moet ik iets anders doen. Daar heb je een coach voor nodig, doe je dat niet dan kom je uit bij bijvoorbeeld Diginotar. Buiten de organisatie, de gevoerde governance wat niet zo wat het zit er in. Dus je cyber controls moeten het wel afdekken. Vandaar dat ik de neiging kreeg om het om te draaien. Gegeven de assessment vanuit een wie is nou waar verantwoordelijk voor en waar wil je

strakke governance op uitoefenen? Dan moet je eerst bepalen wat mag en dan pas krijg je de aanpak. Vandaar de vraag moet het niet andersom (governance en approach in strategische loop).

[*Het strategische gedeelte is gebaseerd op implementatie binnen ERG (Enterprise Risk Goverance). Dus waar willen we naar toe en hoe, gevolgd door de operationele aanpak*]. **De governance ligt nooit meer alleen bij jouw eigen organisatie, dus daarom is governance naar voren gekomen in het model. Stel dat Microsoft nee zegt, wat doe je dan als organisatie in je approach? Dan zit er een gat in je beveiliging.**

[*Is dit niet een activiteit die zit in operationeel/tactisch niveau t.o.v. strategisch niveau?*]. **Dat is juist de valkuil. Daar heeft het wel heel lang gezeten. Dat is een IT vraag, zorg maar dat de leverancier het veilig levert. Maar dat kan niet. Het is geen CIO (Chief Information Officer) verantwoordelijkheid, maar een CEO (Chief Executive Officer) verantwoordelijkheid. Dat is precies het probleem, je wilt het eerder naar voren hebben.**

[*Het framework zoals hier gepresenteerd schept een ideaalbeeld.*]. **Zeker en ik kan inmiddels wel zeggen dat het ideaalbeeld een onrealistisch beeld is. Maar dat heeft heel simpel met wetgevende bevoegdheden te maken**. Ik kan nog zo graag als defensie zijnde willen wat er in Microsoft zit maar dag mag niet. Dat heet intellectueel eigendom (IP, Intellectual Property). Je mag het niet inkijken. Je mag enkel de leverancier vragen dat het veilig is en mocht dat niet het geval zijn dat hij snel handelt. Maar als dat een gegeven is, inmiddels is het een gegeven, zeker omdat de governance discussie naar voren komt. Je kunt nooit meer alleen in control zijn. **Dit model gaat uit van governance in een controleerbaar domein, in een piramide. En de stelling bij cyber is het is nooit meer een piramide. Dus het is een collected governance, het is een andere manier.**

[*De vraag in dezen is ook wat stuurt wat aan? Spreken we van een top-down of bottom-up approach?*] **En dat is op zich ook juist en andersom kan het ook. Maar dat is normaal. Bij andere trends is dat niet anders. Als jongeren iets willen, dan gaat de marketing daarop reageren en die komt met een marketingcampagne. Top-down en bottom-up is een permanent spanningsveld en dat houdt de organisatie ook in beweging. Het enige punt is dat die modellen leunen allemaal op controleerbare doelen (top-down).** En de interessante vraag is wil je het echt helemaal goed doen, dan heb je maar twee mogelijkheden. Of je doet het top-down in je organisatie. Dan moet je alles zelf bepalen, open source. Dan moet je er wel goede jongens neerzetten, maar dat kan. **Of je definieert een andere top. De top is de top der piramiden, dan krijg je organisatie 1, 2 en 3. En dan zeggen we als je dit wil beschermen dan moeten die drie topjes bij elkaar gaan zitten en dan krijg je een collective governance. Dat kan niet anders, ze zitten aan elkaar vast.** Nu heb je bijvoorbeeld de meldplicht, incidenten moeten worden gemeld. Straks krijg je aangiftes. En wie moet er dan handelen? Een andere. Dan is een deel van de governance help mij van die inbreker af te komen een politionele bevoegdheid. Dan heb je weer een andere speler. De governance wordt iedere keer bepaald door de spelers. **Dus eigenlijk heb je twee soorten governance, ecosysteem governance en organizational governance in je eigen domein.** Hier is gegeven wat ik kan en mag doen, mits die andere het ook doet en anders ligt daar het gat. Ik kan als

Justistie zaken dichtzetten, maar dan moet Diginotar dat ook doen. Zo zou je het ook kunnen oplossen dan maak je er een soort van vijftrap van en hang je deze er tussen. Maar het is geen assessment, want het ecosysteem bepalen dat doe je juist hier (strategische gedeelte) dat zijn de spelers en de processen. **En in de technologie as van de piramide daar zitten die zwakheden. Mijn advies zou zijn houdt dit in het cyberdomein. Houdt die processen centraal of je moet hier zeggen primaire processen (cyber). En dan is dit cyber response (response).**

Risk, internal/external. In je onderzoek mis ik de internal risks. Je hebt ze wel, maar je noemt ze niet. Bij Wikileaks classificeerde je een aantal dreigingen. Je maakt een onderscheid tussen hacktivists en terrorists terwijl dat wat wij in de praktijk merken zijn dat wel verschillende groepen. Maar ze hebben eigenlijk een identiek doel. Vanuit het dreigende beeld gezien zijn er twee dingen vergelijkbaar. Ze hebben een zelfde doel onthulling etc. Ze hebben een emotioneel doel, het is een intangible goal. En het tweede is ze gebruiken dezelfde tools. Een terrorist en hacktivist zijn allemaal kleine organisaties. Het is niet een lonesome hacker, het zit daar wel tussen. Ik zie geen verschil, ik heb deze discussie ook met diverse klanten gehad. De hacktivist groep die bombardeert met email die is niet anders dan de terrorist die bombardeert met email.

[*Het doel is hetzelfde enkel de classificatie is anders*]. Ja, je noemt het anders. Ik bekijk het heel erg van hoe adviseer ik organisatie om weerstand te bieden tegen cyber dreiging en dan tot nu toe zie ik geen verschil van hoe een organisatie zich zou beschermen tegen een terrorist en een hacktivist. Het doel is allebei publiek maken van en publiekelijk een bepaalde reactie veroorzaken. Allebei beperkte middelen. Ik zou niet weten wat ik een organisatie anders zou moeten adviseren om zich te beschermen tegen de ene zowel als de andere. Dus vanuit cyber operations technologie zie ik het verschil nog niet echt. Dit was er eentje om mee te geven.

Wat ik miste in je verhaal was de insider threat. Alles wat je hebt beschreven is outsider. Maar de insider hoort hier wel (internal risk). En de case Wikileaks beschrijft wel de perfecte insider threat.

Pas op met de volgorde. Dat heeft met name te maken met de mensen met wie je praat. Als je praat met iemand die uit de defensie hoe komt. Die kent namelijk de volgorde strategic, operational tactical. Dat is bij defensie omgedraaid. Ze bedoelen precies hetzelfde, het is enkel omgedraaid. Dus daar moet je van bewustzijn. Er zijn ook mensen met een defensiepet die naar cyber kijken en doen dit net andersom. Die moet je goed neerzetten en ieder gesprek toetsen van; dit bedoel ik.

[*Hoe creëren we awareness. In combinatie met vervolgvraag, de praktische toepasbaarheid van het model.*]. Dat is een interessante vraag, daar zitten wij momenteel ook mee te

stoeien. Je zou het model dubbel moeten embedden. Dat betekent één embedden in de wetenschap. Dus wie gaat hier straks mee verder. Hoe veranker je dat het model verder wordt gebruikt. Dus embedding in je future research. Deel twee is een stuk lastiger en dat is embedden bij klanten en bedrijven. Je moet beginnen bij de bedrijven die er klaar voor zijn. De bedrijven die zeggen dat is interessant, dat ga ik lezen. Dat is maar een beperkte set aan bedrijven, bijvoorbeeld die onder dreiging staan. Die zijn al aware, bijvoorbeeld ze zijn al een keer bestolen.

De bedrijven moeten er dan straks mee doen. Het lastigste is niet awareness op bedrijfsniveau, maar hoe krijg je de individu aware. De uitoefening van de governance is het moeilijkste advies om aan bedrijven te geven. Want dan maak je het concreet. En dan kom je op een blokkade van niet meer willen.

[*Waar is dat op gebaseerd?*]. Ze voelen de dreiging niet. Vinden het niet interessant. Kost geld. En het kost energie. Hoe dan ook het komt niet aan.

Identity theft is wel één van de weinige knoppen waar je op kan drukken. Dan wordt het al wat vervelender. Want dat is namelijk een individual asset.

[*Is identity theft niet direct gelieerd aan information theft*]. **Nee, information identity is wat anders. Eigenlijk zou je bij risk moeten zeggen theft of IPR (Intellectual Property) en identity theft. Allebei is het informatie maar het doel is anders. Waarom het handig is om ze op te splitsen is dat IPR het individu niet raakt en bij identity theft is het net wat anders.**

In de huidige opzet ben ik het er niet mee oneens, maar vanuit mijn positie is het nodig om het meer op te splitsen. Het is zoeken naar awareness triggers. Ieder bedrijf met IP (Intellectual Property) is bang voor information theft. Fokker met zijn ontwerpen, Shell met waar ligt de olie.

Bij IT sabotage zit je meer in de hoek van de critical national infrastructures. Het hacken van useraccounts vind ik geen IT sabotage. Stuxnet is echte IT sabotage. Het verschil dat ik maak met een DDOS (Denial of Service) attack en een email bom de maken gebruik van bestaande processen. Die vergroten die processen. Het is een bestaand kanaal. IT sabotage is dat je malware installeert of dat je in een domein komt waarbij echt offensieve IT wordt ingezet; de Stuxnet en Flame bijvoorbeeld. En dat is gericht op het saboteren van IT. Bij een DDOS wil niet zeggen dat je IT het niet meer doet, er wordt een extreem knelpunt aangeroepen. En dat is voor mij een andere categorie.

[*Naast de wetenschappelijke embedding streef ik ook naar de sociale relevantie van het onderzoek*]. Als je kijkt naar de economische schade als het gevolg van IP theft dan hoef je niemand te overtuigen. Maar de vraag is je moet er op een dergelijke manier naar kijken dat

het ongebonden blijft. Iedere organisatie die ik benader die beseft meteen tot aan de overheid aan toe dat die grenzen van het governance model, het eigen governance model en het niet controleren van je ecosysteem dat ligt beyond control. Dus die gaan er geen energie in stoppen. Die roepen de leverancier erbij om het te laten regelen. Waar is dan de entiteit in de samenleving die zegt van; misschien moet er dan toch wel een soort van big-brother ecosysteem gaan ontstaan. En wat is dan de impact op privacy? En dat is de wetenschap, die is de enige die dat kan. Het is niet voor niets dat je nu vier Universiteiten aan de gang ziet.

[Zijn er o*verige zaken die ontbreken, hiaten, aanvullingen, suggesties?*]. In principe niet. Het eerste wat opvalt het is wel een goed verhaal. Het staat wel echt stevig.

Expert 7

[*Introductie model*]. Ik wil graag starten met de definities. Je hanteert het onderscheid op het gebied van Information Security, Cyber Security en Cyber resilience. Je geeft aan dat cyber security meer omvat dan information security. Ik ben publicaties tegengekomen die het tegengestelde suggereren. Dat heeft wellicht niet direct invloed op je model, maar wel op de scope van het onderzoek.

Ook nog een vraag, hoe zit cyber defense in relatie met cyber security. Want waar ik naartoe wil is dat in deze plaat cyber security komt als zodanig niet meer terug.

[*De strekking is er wel naar. Dit is te zien bijvoorbeeld bij reputation & assets. CIA voor IS, maar business assets is wel het bredere perspectief*]. Want ik benader het even vanuit de praktijk, ik heb hier nu het model en gekeken naar je literatuurstudie en op basis van het model vind ik het lastig te achterhalen wat de scope is. Als voorbeeld het Ministerie van Defensie heeft in haar cyber strategie nu staat het ontwikkelen van defensieve capabilities. Waar komt dat in dit model terug?

[*Het doel is een generiek model welke handvatten geeft aan managers. Ik kijk niet naar een specifieke aanpak. Maar wel waar je op moet letten op basis van belangrijke factoren*]. **Dit ziet er uit als PDCA (Plan Do Check Act, strategische cyclys). En wat me dan opvalt, is dat je governance in de loop hangt en dat het niet iets is wat over de cyclus heen zit. Is coporate governance niet het überhaupt het stelsel aan maateregelen wat de organisatie treft om te sturen en te beheersen. Volgens mij zijn objectives en directives onderdeel van een governance.**

[*In principe zie ik het model als governance. Dan is de naamgeving zoals ik deze nu hanteer verwarrend.*]. **Wat ik mooi zou vinden aan het model en dat haal ik nu niet uit het model is dat approach iets is van het implementeren van de organisatie in. Als je mij dat niet vertelt, dan zie ik dat niet in het model terug**. [*Voorbeeld getoond van modellen met meerdere lagen (strategisch, tactisch en operationeel)*]. Als ik kijk naar het model en de dimensies (verticaal in een organisatie) die zitten er wel in, maar het zo mooi zijn als dat in het model ook terugkwam, visueel. Je had het net ook over policies en gaf aan dat dit tactisch is, maar voor mij is policies beleid en dat is strategisch. Dus policies voor mij is strategisch. Beleid is schrijven vanuit de top van de organisatie.

En hier ben ik het niet mee eens (piramide model), dat komt misschien omdat ik uit de overheid kom, maar policies op tactisch niveau is niet de wereld waar ik vandaan kom. Ik ben het eens met strategisch, tactisch en operationeel. Echter wat er naast staat niet. Company policies is beleid en dat is strategisch en daar begint het mee. Dat zie ik anders. En daar zit wellicht dan ook de trigger met het model in.

Want wellicht is het taal. Maar als je de strategische loop begint, zou ik voorstellen dat je begint met een policy (i.p.v. objectives en directives). En een policy is onderdeel van een governance, die snap ik. En als ik kijk naar de PDCA dan zit deze deels verwerkt in de strategische loop. Assessment vind ik wel een aardige. Als dit een soort van baseline is maakt dat ook dat je een soort van as-is maakt en een to-be en dat zie je in de meeste cycli niet terug.

En waar ik ook benieuwd naar ben is de vier r'en. Ik hoor je zeggen operationeel niveau, maar waar zit dit op strategisch niveau? [*Dit is een aanpak van de doelen die ik gesteld heb als bedrijf op strategisch niveau*].

De ben ik het nog niet eens met de positionering van operationeel tactisch met betrekking tot het model. Het blok cyber. Welke processen heb je door je bedrijf lopen en welke zijn daarvan kritiek? Wat voor data of informatie gaat daar doorheen en welke wil je daarvoor beschermen en dan de aanpassing op technology. Nu loopt dit allemaal op operationeel niveau. En dan definieer je de response en dat is eigenlijk het tweede wat ik niet zie. Waar gaat de response de organisatiegrens over? Je supply chain. [*Dit zit nu gedeeltelijk in responsibilities en partnering verwerkt.*].

Nu heb ik processen geoutsourced is dit dan mijn probleem? Stel dat er een verantwoordelijkheid van het software-ecosysteem buiten mijn verantwoordelijkheid ligt. Dus hoe tackle je dat met dit model zodat het geen blinde vlek wordt. Dat is het mooie van het model maar wellicht ook het gevaarlijke, ik kan deze nu hangen onder responsibilities, maar hangt deze er ook?

[*Het model kan worden ingezet om potentiële gevaren bij derden te analyseren om zodoende deze af te dichten.*] En als ik zo naar het model zit te kijken verwacht ik ook repositories achter ieder concept. [*Deze zijn nu beschreven in het onderzoek, maar bij eventuele praktische inzetbaarheid is het inderdaad verstandig om daar naar te kijken*].

Bij vulnerabilities zit dus ook een holistische benadering. [*Correct*]. **Dat is een juiste benadering want vulnerabilities gaat meer over dan enkel en alleen bugs in software, de mens speelt hier ook een rol. De awareness van mensen kan ook zo maar een zwakheid zijn wanneer ze dit niet genoeg zijn.**

Wat ik mooi vind, maar mis waar zit nu het proces van het managen van risico's. Risicomanagement is: ik onderken de risico's en ik ga mitigerende maatregelen nemen daardoor treedt een risico niet op. Maar je hebt ook een response van: ik heb risico's gemanaged, maar ik heb een risico niet gezien, het gaat faliekant mis en ik moet naar een actieve respons gaan. Waar zit dat het in het model verwerkt?

[*Het model is niet enkel om branden te blussen, maar ook om voorbereid te werk gaan. In den beginne maak ik geen onderscheid tussen incident management en het mitigeren van risico's (risico management)*]. De voorbereiding zit die ook in de response? Momenteel zit ik in een studie bij NATO. Wij hebben gezegd je het bet een periode dat je om de tafel zit (asessment, approach etc). En dan definiëren we ook een crisis. **En bij het model zie ik dat niet echt terug. Risicomanagement en preventie. Bij een crisis ben je niet zozeer aan het managen maar om een echte crisis te verwerken. En wat ik ook zie is dat in de eerste fase hele andere stakeholders te zien zijn dan wanneer er een echte crisis heerst.**

Risicomanagement is preventie, maar op een gegeven moment moet je ook, zoals je nu in respons hebt echt incidenten gaan managen. En dan is het geen risicomanagement maar incident management en zo verder. Er lopen in respons een aantal processen door elkaar heen voor mijn gevoel. En dan kan het zijn dat we niet hetzelfde beeld hebben.

[*Ik zit op CRG, echter voor het overzicht maak ik geen onderscheid tussen incident en risk management*]. Wat ik mooi vind is het gedachtegoed van de wielen. Hoe zijn deze gepositioneerd? [*Uitleg van de tandwielen op strategisch en tactisch/operationeel niveau*]. **Je wil in de linkerplaat heel veel vertellen. Ik ben wel op zoek naar waar hangt dit samen, waar zit incident managmenet etc. Wat ik vooralsnog mis is de gelaagdheid.**

En Cyber Deterence ben ik ook niet tegengekomen. Het is eigenlijk een voorzorgsmaatregel om ervoor te zorgen dat men twee keer gaat nadenken alvorens ze naar binnen willen komen. In de studie die we bij NATO doen hebben we in de repons over deter. Bijvoorbeeld vanuit de overheid dat je doet aan het platleggen van servers waar botnets op draaien. Dat zou je kunnen zien als deterrence. Ik zou het model ook gelaagd graag zien. En wat ik hier nog te weinig zie is dit ik hier nog de supply chain mis. **En mocht een bedrijf het willen gaan inzetten. Dan moet het model ook zeggen dat het niet eindigt buiten de muren van het bedrijf. En dat zit ergens in de strategie. Van let op je bent van andere mensen afhankelijk.**

[Een voorbeeld wordt getoond van een gelaagd model]. Voor mij wordt het dan visueel duidelijker. Je laat dan ook het speelveld beter zien. Ik denk links een proces te zien maar dat is het niet helemaal. [*Ik zou niet van een proces willen spreken. Het zijn basisbegrippen die er omheen draaien*]. Ik wordt daar een beetje op het verkeerde been gezet. **Ik zie processen maar niet ieder proces bestaat uit activiteiten. En dat is onduidelijk voor mij.** Waar ik modelmatig last van heb is dat ik andere modellen er op plak en dat ik teveel verschillende dingen in één plaat terug zie komen. Daar ben ik vrij snel van af van die last maar ik ben kapstokjes aan het zoeken. Bij risicomanagement zie ik een aantal dingen terugkomen. [..]

[*Ik heb ook niet het verschil gemaakt tussen risicomanagement en incident management*]. Modelmatig zou ik verwachten dat je dat terug zou zien in het model.

[*Voorbeeld van model op basis van risicomanagement*]

Wat mooi is en wat mij zou helpen als onder de concepten een soort van menuutjes staan met eigenschappen van de blokken. Ik merk wel dat bepaalde dingen wel in het onderzoek staan, maar in het model nog niet terug komen.

[*Inderdaad, de gelaagdheid en ook de supplychain*]. Ja, en wat je ook zou kunnen doen is je model zo laten en in een andere weergave tonen hoe het bij een bedrijf er gelaagd uitziet. Wanneer de verschillende concepten op de betreffende niveaus precies terugkeren. En let er dan ook op dat je met partners te maken hebt. Dan hoef je het ook niet in één plaat te vinden. De inhoudelijke governance kun je dan in één plaat vangen. En in de algehele context kun je het in een ander model vangen.

Appendix D – Expert interviewees

First session

Expert interview	Position	Company
Expert 1 – Roy Jansen	Cyber Competence Lead IT & Risk Management	Atos
Expert 2 – Rob Mellegers	Security Principal, Technology Risk IT & Risk Professionals	Atos
Expert 3 – Raymond Bierens	Head of Global PHT Defense and Security Portfolio Management	Atos

Table 16 - Expert interviewees first session

Second session

Expert interview	Position	Company/University
Expert 1 – Herbert Bos	Professor VU University	VU Amsterdam
Expert 2 – Paul Oor	Country Security Officer	Atos
Expert 3 – Rob Mellegers	Security Principal, Technology Risk IT & Risk Professionals	Atos
Expert 4 – Dimitri Belutchkin	Global Portfolio Manager	Atos
Expert 5 – Raymond Bierens	Head of Global PHT Defense and Security Portfolio Management	Atos
Expert 6 – Jo Godderij (input via Expert 5)	Vice President Government Affairs Europe and Africa Atos Global PHT	Atos
Expert 7 – Roy Jansen	Cyber Competence Lead IT & Risk Management	Atos

Table 17 - Expert interviewees second session (validation)

Universiteit Utrecht

Atos