THE STRUCTURE OF A CYBER RISK

A SCENARIO BASED APPROACH IN CYBER RISK ASSESSMENT

July, 2016

Master Business Informatics
Faculty of Science

Floris Delmee
Utrecht University
Deloitte Nederland

Universiteit Utrecht

Deloitte.

Author

Floris Delmee
[3691926]
f.m.delmee@students.uu.nl
Master Business Informatics
Utrecht University

First supervisor

Dr. Floris Bex
Department of Information and Computing Sciences
Utrecht University

Second supervisor

Dr. Fabiano Dalpiaz
Department of Information and Computing Sciences
Utrecht University

Deloitte Supervisor

Bas Maessen
Cyber Advisory
Deloitte the Netherlands

I. ABSTRACT

The growth in the number- as well as the sophistication of cyber risks results into a growing impact of these risks towards organizations and individuals. The growing complexity of- and dependency on IT environments within organizations together with the growth in numbers and sophistication of cyber threats results into a bigger impact of these threats towards organizations and individuals (Adomavicious, Bockstedt, Gupta, & Kauffman, 2008; ENISA, 2013; Pfleeger, Pfleeger, & Margulies, 2015). These complex and sophisticated cyber risks often consist of multiple threat events, which is in contrast with a lot of the risk analysis approaches that are focused towards atomic risks (Barnum, 2014). This misalignment asks for a new approach to capture and assess cyber risks when conducting a cyber risk analysis.

Within this research, a literature review has been performed to identify the different concepts that are relevant within a cyber risk scenario. This review resulted into a set of concepts to capture the story of a cyber risk, which allowed us to include all the relevant (contextual) aspects of the risk. The different concepts are based on various risk analysis methods, and captured within a cyber risk taxonomy. The concepts in the taxonomy include the threat events a threat agent initiates to reach its goal as well as the contextual situation that is relevant for the story of the risk. The contextual elements include the targeted asset and organization, details of the threat agent, the exploited vulnerabilities, applied controls, and an estimation of the business impact. This structure is applied to three different causal models: Bayesian networks, ANRAM, and CORAS (Bex & Hovestad, 2016; Fenton & Neil, 2013; Lund, Solhaug, & Stølen, 2010). These models provided three different approaches to assess a cyber risk scenario.

A quantitative model like Bayesian network could be applied to capture the causal structure of the threat events, as well as the probabilistic dependency between the contextual elements of the cyber risk to determine the scenario's probability. We were in our research however not able to specify these relations into a quantitative network. ANRAM could, in contrast with the quantitative Bayesian network, be used to assess the cyber risks in a more qualitative oriented approach. This model assesses the plausibility and impact of a risk scenario based on the different arguments that attack or support the risk. While this model has a formal logical grounding, it provides a more rudimentary risk assessment, and therefore allows an easier application of the model. The third model, CORAS, is even more qualitative oriented and can be used to support a risk analysis approach or to visualize and communicate the risk scenarios.

The findings of our research propose a structure to capture the entire story of a cyber risk scenario. The proposed structure is captured in a taxonomy and applicable within three different causal models, which could all be used to reach a different goal. A Bayesian network could be used for a quantitative, and detailed, probability estimation of a cyber risk scenario. ANRAM should be used during a risk assessment where less detailed information is available, or where the needed result of the assessment does not require a high level of detail. The third model, CORAS, could best be applied if a quick overview of the scenario for communicative purposes is needed.

Keywords: Cyber risks, Risk scenario, Causal modeling, Scenario based risk assessment

II. PREFACE

This master thesis represents a lot of hours of hard work and dedication towards an interesting topic, which is the fast developing world of cyber risks and security. An interesting topic where the 'good guys' are challenged on a daily basis to prevent and control the various cyber risks and threats that are initiated towards them. This challenge, and need for new and innovative ideas together with the close alignment between the business and IT aspects in cyber security is what captured my curiosity towards this topic.

Now that my thesis is almost finished I would like to thank my supervisor, Floris Bex, for all his help during my graduation research. He supported me through some difficult phases of this thesis, and I appreciated his help in providing clear and structured arguments within my thesis. Besides Floris, I would like to thank Fabiano Dalpiaz for his contribution in reviewing this thesis as my second supervisor. Besides my supervisors I would like to thank the Whatsapp group: "Scriptie fun", for its high levels of sarcasm and jokes to share our joy and troubles during our combined graduation thesis experiences. And of course, not to forget: I would like to thank my girlfriend, for her mental support during this period, as well as the textual and grammar checks of various parts of my thesis.

I have performed this graduation research as an intern within the Cyber Advisory department of Deloitte. The pleasant atmosphere, and helpful and friendly colleagues helped me to further expand my knowledge and interest towards this topic. I would like to thank all of the colleagues, and provide a special thanks towards my daily supervisor: Bas Maessen. His way of working, helpful tips, and contributions were of great value to me during my research and increased my overall problem analyzing skills.

Now, after a period of almost nine months since the original idea for my thesis was born it is coming to an end. Although this preface is the final part of the thesis that I have written, I am vigilant to say that I am really finished until I have submitted the entire thesis. This vigilance is mainly caused by the many warnings I have received about the final stage of writing your thesis. Despite these warnings it turns out I am still able to finalize my thesis in a timely manner (even with playing maybe too much games of pool during my Deloitte internship...), and maybe more important: I am finalizing it without losing my positive state of mind.

Have a great read, Floris

Amsterdam, July 2016

III. TABLE OF CONTENTS

IV. LIST OF FIGURES

V. LIST OF TABLES

1. INTRODUCTION

The rapid development of innovative technologies provides a lot of opportunities for organizations and governments (Choo, 2011). A consequence of this rapid development in possibilities is the growth in complexity of the IT landscape (Adomavicious et al., 2008; ENISA, 2013; Pfleeger et al., 2015). This complexity, which is increased by the interconnectedness of computers and systems such as the Internet of Things (Information Security Forum, 2015; Verizon Enterprise, 2015), results in a higher dependency of people and businesses on a proper functionality of these technologies. Due to this higher complexity and dependency a new and large set of IT- and cyber related risks is introduced. These risks allow a growth in cybercrime related activities. This crime, which is becoming more sophisticated as well, can be seen as a profitable one since the returns are great, and the risks for cyber threat agents are relatively low (Choo, 2011; McAfee, 2014). The annual cost of this growing crime industry to the global economy is estimated at $400 billion (with a range between $375 billion and $575 billion), which is comparable to the financial impact of the illegal drugs industry (McAfee, 2014). The growth of this already large industry as well as the varied and growing cyber threat landscape (Choo, 2011) asks for more and better ways to control or mitigate these risks.

This research takes a closer and more detailed look at the above mentioned cyber threat landscape, by focusing on the different scenarios of the risks that exist within this landscape. A risk scenario represents the causal structure, and the probabilities of the different events within a risk. These events represent the triggers that could cause a risk to occur, the impact on the organization resulting from the risk, as well as the applied mitigation, and control tactics. There are a number of risk analysis methods available (Eloff, Labuschagne, & Badenhorst, 1993), which all have different approaches to identify, describe, and estimate a risk (Rausand, 2011). The risk concepts within a risk scenario are based on those existing risk analysis approaches. The concepts together will form the basis of the proposed cyber risk taxonomy. The taxonomy describes a cyber risk scenario in various levels of detail. The basis of the taxonomy to capture cyber risk scenarios is based on Fenton and Neil (2013), who proposed a general risk scenario that consists of one or more trigger events that cause the risk and certain consequences. This general structure of a risk scenario is elaborated with cyber risk concepts to construct a cyber specific risk concept. A general risk analysis is, besides the identification of the events within the scenario, needed to determine the severity of each scenario. This analysis includes an estimation of the probability values of the events, such as the chance that a phishing mail is opened by an employee, within the scenario. Another part of the analysis will reveal the business impact caused by the cyber risk (e.g. a loss of competitive advantage due to stolen intellectual property).

The taxonomy together with the probability- and impact estimations will be captured in an existing causal model to further analyze, structure, and present the causal structure within the cyber risk scenarios. The model can, besides the risk estimations, be used to capture the dependencies of the risk within the cyber risk scenarios in a structured manner. This structured data facilitates the reuse of cyber risk knowledge during a cyber security analysis.

1.1 PROBLEM STATEMENT

Cyberspace provides a lot of opportunities for organizations and governments, but alongside those opportunities cyberspace poses a lot of threats (Choo, 2011). The amount of cyber risks grows alongside the sophistication of those cyber risks (Beggs, 2010; Ponemon Institute, 2015). This combination, together with the sophisticated cybercrime industry strengthens the need for proper cyber security. This security, in the form of advice, is provided by several consultancy companies, such as Deloitte, KPMG, or EY. However, the given advice is mainly reliant on the tacit knowledge and experience of specific experts and specifically tailored to the client's situation. The deliverables, which provide a good overview of specific cyber risks towards an organization, are often unstructured and difficult to reuse in a new project. But such reuse could result in the generation of a better overview of the cyber threat landscape within the organizational memory. Nonaka (1994) identified four modes of organizational knowledge creation. This included the translation from individual 'tacit' knowledge towards structured 'explicit' knowledge. This structured knowledge can then be combined into new, or extended knowledge (Nonaka, 1994). By providing this structure, and allowing the combination of knowledge, it becomes possible to create a better overview and understanding of the cyber threat landscape. This overview is essential to make correct decisions about controlling or mitigating the threats for a specific organization (Choo, 2011). A clear structure to analyze and model cyber risks can provide the needed overview and the ability to share this overview. Current cyber knowledge sharing approaches are however often based on atomic information that lacks sophistication and expressivity (Barnum, 2014). It is therefore needed to include a clear understanding of the business impact and its relation to the threat events within the cyber risk scenario that caused this impact. By capturing these relationships in a structured manner, it is easier to reuse (parts of) the scenario to create new scenarios and use them in future projects.

The needed structure of cyber risks could be provided by identifying a cyber risk taxonomy that captures the causal structure of the cyber risk as well as the probability values and the business impact. This causal structure is needed since a risk almost never consists of just one event, but rather of a combination of several events. These events together cause the risk as well as several events that result from the risk and determine the business impact. An advantage of such a structure is the possibility to identify multiple events that can be adjusted to control the risk or mitigate the business impact (Fenton & Neil, 2013). Although there are several methods to perform a risk analysis (Eloff et al., 1993), there is no method that provides a taxonomy to capture cyber risk scenarios.

The cyber risk scenario taxonomy can be elaborated with a model to calculate the probability values as well as to represent the causal structure in an understandable manner. The CORAS model based security analysis (Lund et al., 2010) provides an approach to model the structure of security risk scenarios. The focus of the CORAS model is however more on the communication of the scenarios than the estimation of the probability and impact estimations (Braber, Hogganvik, Lund, Stølen, & Vraalsen, 2007). More general modeling techniques, like Bayesian Networks (Fenton & Neil, 2013; Rausand, 2011), Influence diagrams (Howard & Matheson, 2005; Shachter, 1986), Bow-Tie model (Fenton & Neil, 2013; Rausand, 2011) or the ANRAM model (Bex & Hovestad, 2016) based on the Hybrid theory (Bex, 2011)) have the potential to model cyber risk scenarios together with the probability- and impact values. These models however do not include cyber risk specific concepts in their models. More detailed advantages and disadvantages should be identified to select the best fitting model(s) to capture and model the cyber risk scenarios.

1.2 RESEARCH QUESTION

The problem statement above requests a taxonomy to structure cyber risk scenarios as well as an approach to estimate the impact and probability values. This research, which addresses that need, is based on the following research question.

What are the causal structures and the probabilities of typical cyber risk scenarios, and how can these be modeled and captured in a taxonomy?

The goal of this research is the development of a structure to capture cyber risks scenarios. This structure will be defined in a taxonomy, which is based on cyber risk specific concepts gathered by conducting a literature study towards risk analysis approaches and expert interviews at Deloitte. The identified taxonomy is captured within one or more existing modeling languages to represent the causal structure, probability, and resulting impact of the risk scenario. To determine these values, it is necessary to identify a structured approach to determine both the probability and the impact of a cyber risk. This approach is explained in Chapter 2, which describes the approach and design of this research.

1.2.1 SUB RESEARCH QUESTIONS

The answer of the main research question will be based on the following seven sub research questions. For each sub research question the relevance towards the main research question is described.

1. **Which steps and approaches are performed within a risk analysis?**

A literature study towards existing risk analysis approaches will be conducted. This study will provide valuable insights in the different, and relevant, aspects of a risk that need to be identified and described. These analysis approaches, besides the identification of risks, usually include a risk estimation approach. The different risk analysis approaches and methods are described in Chapter 3.

2. **What are possible probability and impact estimations within cyber risk scenarios?**

The aim of this sub research question is to identify the different approaches to determine the probability and the impact of a risk scenario. These approaches are based on existing risk analysis methods that are identified via the first sub research question. This question focusses on the different impact and probability approaches. These approaches are described in Chapter 3.3, and applied to the proposed cyber risk models in Chapter 7.

3. **What are the different concepts within a risk scenario?**

To construct a risk scenario, it is necessary to identify the different concept that construct such a scenario. These concepts are gathered by conducting a study towards the different, existing, ways to capture or model a risk scenario in a structured manner. This study is complemented with the general risk analysis literature study that was conducted to answer sub research question 1. The findings of these studies are described in Chapter 4.

4. **What are the recent developments within the cyber threat landscape?**

An overview of the cyber threat landscape provides more context about the cyber risk aspects of this research. The study towards this threat landscape includes the general developments in the landscape, as well as the known threats, threat agents, and the ways to control these threats. The findings of this study will be described in Chapter 5.

5. **Which existing cyber risk categorizations can be used to categorize cyber threats within a cyber risk scenario?**

There are several different threats within the cyber threat landscape. These cyber threats can be categorized within several existing categorizations. Based on this research question a study is conducted to identify different categorization approaches in both the scientific as well as non-scientific literature. The findings of these categorizations will be described in Chapter 5.2 and applied to the proposed cyber risk taxonomy in Chapter 6.

6. **How can a cyber risk scenario be captured in a structured manner?**

The identification of a cyber risk taxonomy, which is part of the main research question, is addressed by this sub research question. The answer of this question is based on the answers of the third and the fifth sub research question. The different concepts about existing cyber threats will be captured in a structured manner. This structured manner, which will determine the taxonomy, together with general steps to create a scenario is described in Chapter 6.

7. **How can existing causal risk models be used to model cyber risk scenarios?**

The last part of the main research question that needs to be addressed is an approach to model the cyber risk scenarios. The model should capture the probability values together with the causal structure of the risk scenario. This question is answered by applying the, in the previous question identified, taxonomy towards a causal modeling technique, which are identified in the literature study of the third sub research question. A description of the needs of this model, together with a description of the applied taxonomy in the causal models is described in Chapter 7.

1.3 SCOPE OF THE RESEARCH

The aim of this research is to deliver an approach to capture and model cyber risk scenarios. The modeled scenarios will be based on a taxonomy that represents a complete risk scenario. The model should provide an explicit and clear overview of the causal structure of the risk. This structure indicates the chain of events that lead towards the risk, and eventually the impact it caused to the business. The identification of this model will be based on qualitative research, which consists of a literature study, unstructured expert interviews and a validation. Although the validation includes the gathering and capturing of cyber risks in the proposed taxonomy, it is not in the scope of this research to gather enough cyber risk data to perform a quantitative research towards the probability and impact estimations of these risks and risk scenarios. The gathered data will be used in a qualitative manner to validate the structure of the proposed taxonomy's concepts and variables.

1.4 RELEVANCE

The social and scientific relevance is discussed in this paragraph. The social relevance is related to the contribution of this research to society. The scientific relevance is based on the research elements in the

study and the contributions towards the current scientific field. Both the social- and the scientific contributions are described below.

1.4.1 SOCIAL RELEVANCE

A structured approach to analyze the impact and probability of a risks will provide a better understanding of the organization's specific cyber threat landscape. This understanding is essential to make informed decisions about security investments to control cyber risks (Choo, 2011). These decisions are becoming more important due to the growth of more sophisticated cyber threats within the threat landscape (Beggs, 2010), which causes a growing amount of money that is invested in the recovery from- and prevention of these cyber threats.

The modeled cyber risk scenarios will provide an overview of the causal structure of cyber risks within the threat landscape. This causal structure will allow the identification of the dependencies between the different events in a risk that can be controlled or mitigated. This is necessary, especially in the case of a cyber risk, since a cyber risk is not a single event, but rather a chain (or combination) of events that will cause a negative impact (Barnum, 2014). An advantage of this structure, once it is identified, is the possibility to make better informed decisions about the money that will be invested in controlling and mitigating a certain risk. With the identified causal structure, it is possible to target the specific events that cause the risk or business impact.

1.4.2 SCIENTIFIC RELEVANCE

This research's contributes to science in two ways. First a cyber specific taxonomy is proposed to capture and model cyber risk scenarios. This taxonomy is based on the combination of several risk analysis methods together with the characteristics of cyber risks into an approach to structure and capture cyber risk scenarios. The taxonomy is applied to existing causal models. These models provide the ability to capture and assess a broad range of complex risk scenarios to capture the dynamic and complex risks scenarios caused by the equally dynamic and complex IT-products (ENISA, 2013).

The second contribution is that the proposed model can be used to capture risk scenarios. This allows the structuring of cyber risk data, which is needed given the limited amount of available structured cyber risk knowledge (Byres & Lowe, 2004). Such a model can, even though it is not within the scope of this research, capture several cyber risk scenarios in a structured manner and therefore create a repository of structured cyber risk data. This repository will allow further research towards these cyber risks and the general threat landscape.

2. RESEARCH DESIGN

The design of the desired taxonomy to structure cyber risk scenarios will be identified and developed in line with the design science framework of Hevner (2007). The design science framework consists of three cycles: a relevance cycle to align with the needs of the environment, an internal design cycle between building and evaluating the design, and a rigor cycle to align with the (scientific) knowledge base (Hevner, 2007).

The scientific rigor will be provided by a literature review on the different relevant topics within the research (see Chapter 2.1.1). This knowledge will be extended with several unstructured expert interviews at the cyber security department of Deloitte, the organization that facilitates this research. These interviews will provide insights in the current cyber risk environment and the needs of cyber risk analysts, and therefore provide this research with the needed social relevance. Chapter 2.1.2 provides more insights in the different interviews that will be conducted. These two sources, together with the current cyber security practices of Deloitte (Chapter 2.1.3) will result into the cyber risk taxonomy. This taxonomy will be designed in an iterative way as proposed by Hevner (2007).

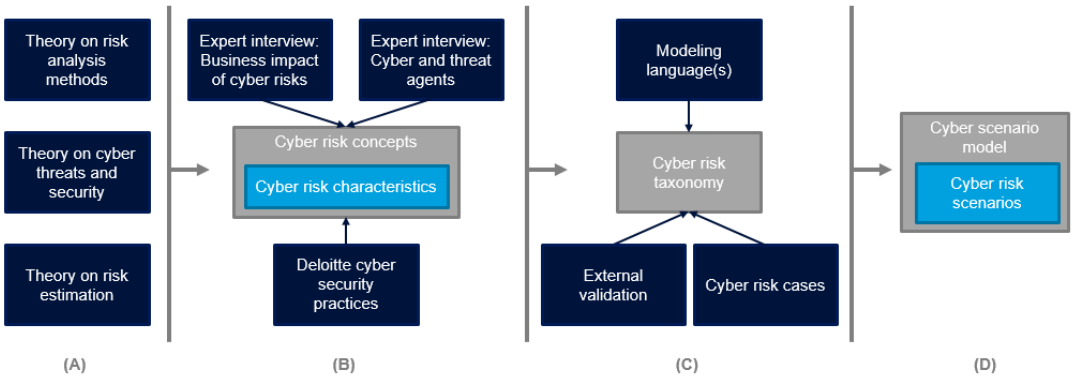

Figure 2.1: Research framework adapted from Verschuren and Doorewaard (2010)

A more detailed design of the research is provided by the research framework of Verschuren and Doorewaard (2010). This framework, of which a tailored version is provided in Figure 2.1, describes the general steps in the research. This research is, as indicated in the framework, divided into four parts. At first a theoretical framework is constructed (column A). This framework consists of scientific literature on risk analysis methods, risk estimation approaches and cyber security, which is gathered via a snowballing principle as described by Wohlin (2014). The scientific literature together with expert interviews and the current Deloitte cyber security practices will result into a set of cyber risk concepts to create a scenario. This step in the research is captured in column B.

As visualized in column C, the cyber risk taxonomy is developed to capture the cyber risk concepts. The taxonomy is further elaborated into a cyber scenario model (column D). This step is performed after external validation interviews with cyber security experts towards the business application of the taxonomy are conducted. This validation is elaborated with a data based validation. The data validation is performed by

capturing several cyber risk incidents in the defined taxonomy. The cases are gathered from an internal cyber case repository of Deloitte (Chapter 2.1.3). Combined, these two approaches result into a validation that is both focused on the situation of the real world (the cyber cases) and the needs of the real world (validation interviews). The validated taxonomy is elaborated by applying existing modeling languages to construct the cyber scenario model that is displayed in column D.

2.1 KNOWLEDGE BASE

The knowledge base that is constructed in this research consists of a literature review, expert interviews and information about the Deloitte cyber security practices. The literature review corresponds with column A of the research framework in Figure 2.1. The Deloitte cyber practices and expert interviews, which are displayed in column B of the framework, will be used to supplement the gathered information and to determine the final cyber risk characteristics.

2.1.1 LITERATURE RESEARCH PROTOCOL

As mentioned above, the literature research will be conducted following the snowballing principle. This principle entails an exploratory search towards relevant literature by further investigating the sources of relevant books and articles (Wohlin, 2014). The search criteria are based on the research topics that are described in the research framework (Figure 2.1). Besides the scientific literature the knowledge base is expanded with non-scientific literature. These sources include research reports and security standards (e.g. NIST, 2014; OWASP, 2015a; Ponemon Institute, 2015).

RISK ANALYSIS METHODS

Literature about general risk models and analysis methods will be used to identify the needed risk characteristics to construct a risk scenario as well as the approaches to determine them. This is done by comparing risk analysis methods (see Chapter 3 Risk analysis). Based on the findings of the comparison different characteristics are identified which, if needed, are expanded with cyber risk specific characteristics to propose an answer towards the first sub research question. This research towards analysis methods will include a research towards risk modeling, which includes the investigation and description of existing causal models that could be applicable to model the different steps within the cyber scenarios.

UNDERSTANDING OF RISK ESTIMATION APPROACHES AND MODELS

Impact and probability estimations are often used to determine the risk value. Existing literature provides several approaches to determine these values. These approaches range from quantitative (and semi quantitative) approaches to qualitative approaches. Quantitative approaches calculate exact probability and/or impact values of a certain risk. These values could be based on historical data. A qualitative estimation is often based on characteristics that have a known impact on for instance a risk (e.g. the skill level of a hacker or the overall awareness of the employees towards cyber risks). Both of the above mentioned approaches are, due to the lack of reliable, structured historical data on cyber risks (Byres & Lowe, 2004), investigated.

CYBER THREAT LANDSCAPE AND CYBER SECURITY

An overview of the most occurring cyber threats within the current cyber risk landscape will be necessary to answer the second sub research question. Scientific research on cyber risks is mainly focused on either a case study or specific techniques and methods to counter cyber threats. Therefore non-scientific reports are included in this research (e.g. Information Security Forum, 2015; Ponemon Institute, 2015; Verizon Enterprise, 2015). These reports provide insights in the most occurring cyber risks as well as insights in the

impact of those cyber risks. The combination of these sources will provide an overview of the cyber threat landscape and some details on the individual cyber risks.

A literature study towards cyber resilience approaches is conducted to complement the desired risk models with controls and mitigations. This literature study is focused on the identification of existing tactics or methods to perform those mitigating or controlling measures over specific control approaches for specific cyber threat occurrences.

2.1.2 UNSTRUCTURED EXPERT INTERVIEWS

Several unstructured interviews will be conducted to extract knowledge from the cyber advisory department of Deloitte to complement the literature research. There are, as indicated in the research framework in Figure 2.1, two interview topics: the technical- and the business aspect of cyber risks. The interviews are used as inspiration and input for further literature research. The findings are therefore indirectly used within this research.

TECHNICAL ASPECT OF CYBER RISKS

A lot of domain knowledge on the topic of cyber security and cyber threats is available within the cyber risk department of Deloitte. This knowledge will be extracted via interviews that focus on the specific characteristics of a cyber risk and the different approaches of cyber threat agents. An important aspect of these interviews is to expand our knowledge base with (non-) scientific literature about these topics.

BUSINESS ASPECT OF CYBER RISKS

The business impact of a cyber risk entails different topics. There are, besides the different aspects of the business impact, several different approaches to determine this impact. It can for instance be expressed in monetary values in terms of losses (Suh & Han, 2003), or as a failed regulatory compliance or caused reputation damage (e.g. NIST, 2012; OWASP, 2015a). The goal of these interviews is to identify which methods/approaches are used in practice, and what their advantages and disadvantages are.

2.1.3 DELOITTE CYBER SECURITY PRACTICES

Besides the input received via qualitative interviews this research is supported with internal documents and practices of Deloitte. This includes an internal cyber case repository, the white hat hacking services and Red Hatting practices, and the cyber resilience framework to assess the cyber security of an organization. These elements will be described in more detail in Chapter 5.5.2, and are used as input for the cyber risk taxonomy.

INTERNAL CYBER RISK REPOSITORY

There is an internal Deloitte risk repository to provide an overview of occurred cyber risks. For each case a description of the organization, industry, attack category, scenario description, attacker's motivation, used techniques, and business impact is described. Within the repository 40 different cyber cases are described. These cases are spread over various industries and are initiated by various threat agents. These cases provide a good overview of the possible impact of cyber risks as well as the risk scenario.

The aim of this repository is not to provide a representative sample of the cyber threat landscape, but instead to provide real examples of possible cyber threats and. This data will therefore be used to test the completeness of the taxonomy as well as the ability to model risk scenarios, but not to provide a complete overview of the current threat landscape.

DELOITTE HACKING PRACTICES

Deloitte provides hacking services and Red Hat operations. These operations test the cyber security of organizations on request and deliver valuable insights. The gathered insights of these departments could provide an overview of the different possible cyber threats and as the success rates of attacks of those threats. The provided hacking services include: penetration tests of networks and systems, phishing tests, and tailored targeted hacking attempts.

The aim of the above mentioned Red Hat team is to provide a client with new insights in possible security flaws. This goal is achieved by demonstrating possible ways in which a threat agent (e.g. hacker or script kiddy, see Chapter 5.4 for more information on the different threat agents) could exploit certain security vulnerabilities to achieve a certain goal (e.g. steal privacy sensitive information or the organization's intellectual property). They make use of high-level attack scenarios as a starting point to think as a threat agent and identify ways to exploit the vulnerabilities of an organization. These scenarios, as well as their experience, will be valuable input for the risk taxonomy and model.

CYBER RESILIENCE FRAMEWORK

Deloitte has an internal developed framework to assess cyber risks, this framework is based on NIST (2014), ISO /IEC 27001 (2013), and the SANS Institute (2015). An advantage of this framework is the mapping between the cyber capabilities of a client, the business processes, and a general threat landscape. The approaches that form the basis of this framework can be used in the proposed model of this research. The framework provides knowledge about different threat agents, motives, assets they target, possible impacts, and a collection of twelve cyber threats. These insights, together with the proposed approach of the framework will be further investigated and described in Chapter 5.5.1.

2.2 FROM A TAXONOMY TOWARDS A SCENARIO MODEL

The taxonomy that represents a scenario and its characteristics are based on scientific- and non-scientific literature, expert interviews, and Deloitte cyber security practices. The concepts of a cyber risk scenario can best be explained as an extended and tailored version of a standard risk event (see Figure 2.2) that consists of a certain threat (trigger) which results into a risk and has a certain consequence (Fenton & Neil, 2013).

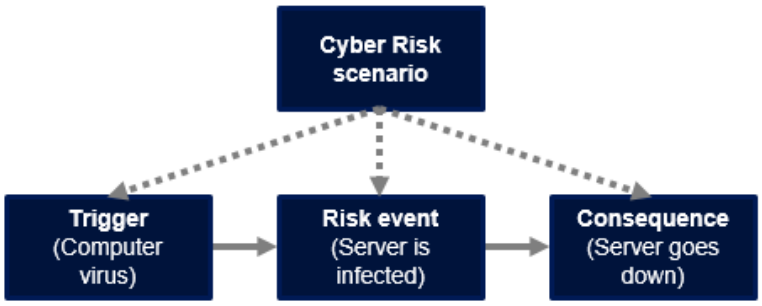

Figure 2.2: Structure of a risk (Fenton & Neil, 2013)

The taxonomy of this research will extend the structure of Figure 2.2 with cyber risk specific characteristics. This will result into a more complete structure to represent a cyber risk and allows for a better estimation of the risk probabilities and the resulting business impact. An example of how the structure of Figure 2.2 can be elaborated towards the structure of a security risk (Lund et al., 2010) is provided Figure 2.3. The list of risk concepts is further elaborated in Chapter 4.2. These concepts are further elaborated towards the cyber risk taxonomy in Chapter 6.

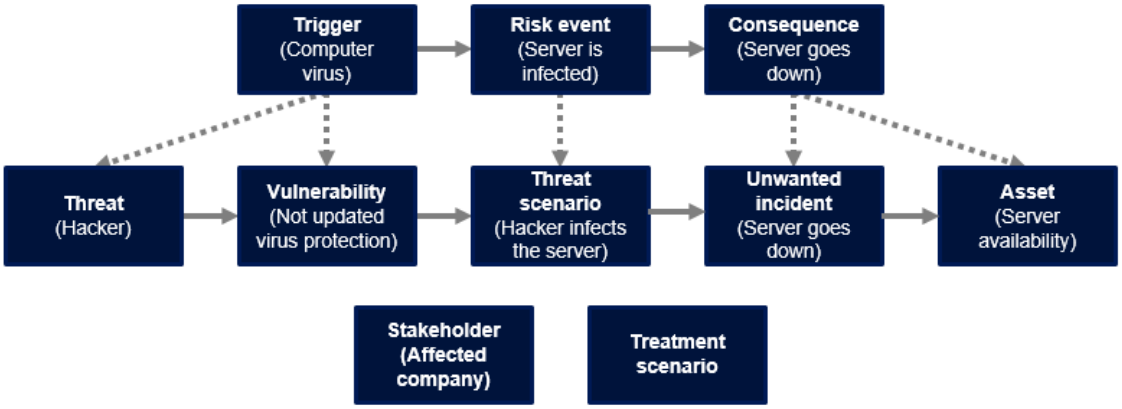

Figure 2.3: An elaborated risk structure towards a security risk (Lund et al., 2010)

The identified taxonomy will be captured in an existing model to represent the causal structure and to allow the modeling of cyber risk scenarios. Besides the structure, the model should be able to represent probability estimations of the individual events (e.g. the probability that someone opens a phishing mail) as well as an indication of the impact of the entire risk scenario. Further requirements of the model to capture the taxonomy are identified in the literature review and defined in Chapter 7.1.1. The literature review identifies several causal models. Three models are selected to capture the cyber risk taxonomy to model a cyber risk scenario. This final step of this research is described in Chapter 7.

2.3 VALIDATION

As indicated in column C of the research framework in Figure 2.1 the taxonomy is both validated with external interviews and data validation. The data validation is conducted by capturing several occurred cyber risk incidents in the taxonomy. This provides an overview of the applicability of the taxonomy towards the real world. The cyber risk cases are gathered from the Deloitte cyber case repository (see Chapter 2.1.3). A more detailed description of this validation approach, together with an overview of the findings is described in Chapter 8.2.

The validation interviews are conducted with different cyber security experts of different organizations. The interviews are aimed towards the social relevance of the proposed cyber risk taxonomy (the first cycle of Hevner (2007)). During the interviews the applicability of the taxonomy within the organization is validated. The validation protocol is provided in Appendix F, the validation results in Chapter 8.1. The combination of these two validation approaches results into a taxonomy that is both validated towards the needs of the real world (the interviews) and the situation of the real world (the cyber risk cases).

3. RISK ANALYSIS

The focus of risk management is to identify relevant risks and provide proper treatment to control these risks and minimize the expected loss due to occurring risks (IRM, 2002). An essential part of risk management is the identification and estimation of the relevant risks. These two parts are addressed in the risk analysis phase of risk management. This chapter describes the different approaches to perform a risk analysis. These approaches are divided over three steps within a general risk analysis. These steps are, according to the Institute of Risk Management (IRM, 2002), as follows:

1. Risk Identification
2. Risk Description
3. Risk Estimation

This chapter describes all three of the above mentioned steps in more detail, these descriptions are based on, parts of, various existing risk analysis approaches and methodologies. The described approaches and methodologies are tailored towards the analysis of IT- and cyber related risks. Each of the sections of this chapter describes one of the above mentioned steps within a risk analysis.

3.1 RISK IDENTIFICATION

The risk identification step in a risk analysis identifies the exposure of an organization towards threats. A risk identification should be approached in a methodical way to ensure that all the possible risks are identified (IRM, 2002). NIST (2012) identified three general approaches to identify risks. An organization can perform a threat-oriented approach which will focus on the threat sources and possible threat events. These events will be translated into threat scenarios that provide the vulnerabilities as well as the impact of these events (NIST, 2012). The second approach is the asset/impact-orientated approach. This approach identifies the most critical assets and the impact or consequences when these assets are harmed via possible cyber threats. The result of this approach includes an overview of possible threat events and the resulting impact. The third approach is vulnerability-oriented, which starts with identifying the exploitable weaknesses in the organization. Based on these weaknesses in the information systems threat events are identified (NIST, 2012). Pfleeger, Pfleeger, and Margulies (2015) indicate that an organization should identify the assets, systems vulnerabilities, as well as the most likely threats to understand the nature of its cyber security. They therefore argue that it is needed to use all three of the approaches for a complete analysis. This section addresses each of these approaches to identify risks. A fourth approach, risk related knowledge sharing, is added in this section and described in Section 3.1.4.

3.1.1 THREAT-BASED APPROACH

The threat-based approach identifies the threats by looking at all the possible risks and known threat agents. According to OWASP (2015a), who proposed a six step methodology to rate risks, it is important to gather information about the threat agent. Four categories of information about this agent should be gathered: its skill level, its motive, the opportunity, and the size. OWASP (2015a) provides an approach to rate the threat agent on these four categories.

Karabacak and Sogukpinar (2005) as well as the IRM (2002) indicate the importance of the identification of possible threats by investigating these threats and becoming aware of the problem. They both however do not provide a structured approach to identify the threats within the threat landscape.

3.1.2 ASSET-BASED APPROACH

The asset-based approach focusses on the identification of different important assets. Based on these assets are the most crucial threats towards the organization identified. Franqueira, Tun, Yu, Wieringa, and Nuseibeh (2011) proposed the RISA (Risk assessment in security argumentation) method to identify and assess risks based on the needs of the software system. This approach, which is based on the framework of Haley, Laney, and Moffett (2008), identifies the most crucial systems as well as possible failures of those systems. The importance of the systems is based on the functional requirements and the underlying goals of the system.

Another approach that identifies the most important assets is the method of Suh and Han (2003). They propose a method to estimate the cost of cyber risks towards an organization. This estimation is based on the value of the damaged assets and the lost income due to unavailability of those assets. The identification phase therefore starts with a thorough investigation towards the organizational business model, processes, and assets. The relative importance of the processes and assets will be determined to identify the most crucial assets. A further investigation towards the probability of the identified risks is needed to complete the risk identification and proceed towards the description and estimation phase (Suh & Han, 2003).

3.1.3 VULNERABILITY-BASED APPROACH

The Failure Modes, Effects, and Critical Analysis (FMEA or FMECA) is one of the first reliable system analysis methods to identify all the possible failures (Rausand, 2011). As the name of the method indicates it is aimed at the identification of all the vulnerabilities in a system. Their approach is based on three general steps: plan and prepare, system breakdown and functional analysis, and the identification of the failure modes and causes. A similar approach to identify potential threats by investigating the systems functionality and weaknesses is HAZOP (Hazard and Operability) studies. HAZOP studies is a systematic hazard identification process that identifies all deviations and potential hazards in the systems functions and decides if any actions are required to control these hazards (Rausand, 2011). A HAZOP analysis is often performed during several meetings in which brainstorm sessions are performed. These brainstorm sessions should be guided with predefined guidewords, and will result into a list of possible threats towards the systems design.

Another approach to identify risks is provided by the cyber security framework of the National Institute of Systems and Technology (NIST, 2014). Their framework provides guidance in the development of the cyber security of an organization. The approach of NIST (2014) is similar to a gap analysis which compares the current state of cyber security towards the desired state. This gap analysis will result into vulnerabilities in the current security of the organization.

3.1.4 RISK RELATED KNOWLEDGE SHARING

In contrast with the above mentioned approaches an organization could use shared risk knowledge to identify relevant risks towards its organization. Several risk related knowledge sharing approaches exist. This section describes the sharing approaches within the context of cyber risks.

Barnum (2014) identified that most risk sharing approaches are human-to-human or via unstructured or semi-structured descriptions via web-based portals or encrypted mails. Besides this unstructured knowledge sharing approach is the knowledge that is shared often focused on individual indicators, instead of the entire

risk scenarios (the next chapter will further elaborate about risk scenarios). There are however several approaches that include more structured cyber knowledge sharing (Barnum, 2014; Dandurand & Serrano, 2013; Verizon Enterprise, 2016). The aim of these approaches is to provide a better overview of the risks within cyberspace. The VERIS framework, initiated by Verizon, is an open accessible project to capture data breach incidents. The aim of VERIS is to provide a way for organizations to both report and look up data breaches. The data structure as well as the data itself is freely available online, the data visualizations capabilities are however still in development.

Knowledge sharing between organizations could be achieved via the Trusted Automated eXchange of Indicator Information (TAXII) (Davidson & Schmidt, 2014). TAXII is a standard that can be used to share sensitive knowledge in various ways. Sharing this knowledge is conducted via producers and consumers via three different architectures. The first architecture is a source-subscriber architecture, which works via one general producer of information, and several consumers. Second, the hub-and-spoke architecture, which includes one central clearinghouse which distributes the information between the different consumers. The last architecture is a peer-to-peer network. This indicates that each organization will share his knowledge directly with the peers within his network. Besides these sharing architectures, there are four different sharing methods possible within TAXII. A consumer can make use of a pull request, where he will only receive information on his own request. On the other hand, there is a push method, which allows the producer to push all the created information towards the consumer. The last two methods are discovery and query. Discovery indicates that each consumer can search within all the shared knowledge, and query indicates that a consumer will only receive the information that matches his query. The different architectures and methods within TAXII allow for tailored knowledge sharing that suits the needs of a specific organization.

Table 3.1: The STIX components (Barnum, 2014)

STIX architecture:	Description
Cyber Observables	Can be seen as the 'base' construct within the architecture (e.g. information about a file name, registry key value, or service)
Indicators	Specific patterns or contextual information that indicate a possible attack
Incidents	The specific instances that affect an organization
Adversary Tactics, Techniques, and Procedures (TTP)	This includes attack patterns, malware, exploits, kill chains, tools, infrastructure, and/or victim targeting
Exploit Targets	This includes vulnerabilities, weaknesses or configurations
Courses of Action	This includes incident response or vulnerability/weakness remedies or mitigations
Cyber Attack Campaigns	This campaign describes an attacker that is performing a TTP or initiates an incident
Cyber Threat Actors	The malicious actor that initiated the attack

One of the requirements of knowledge sharing that have been mentioned in the beginning of this section by Barnum (2014) is to provide structured information that entails the entire problem. Where the overall problem could be captured by creating the scenario of the risk ((De Kock, 2014), further elaborated in Chapter 4), provides the Structured Threat Information eXpression (STIX) a language to describe cyber related attacks (Barnum, 2014). STIX allows a user to capture all the relevant elements in a structured manner. The aim of this language is to enable a system to automatically process the cyber threat information in for instance a monitoring or threat response system. Besides the automatic processing, it is a requirement

of the language to keep it understandable for humans as well. The different concepts from the STIX language are provided in Table 3.1.

The Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) is another approach to enable the knowledge sharing of cyber risks (Dandurand & Serrano, 2013). CDXI can be seen as a knowledge management tool specifically for the cyber security domain. The aim of CDXI is to facilitate information sharing, enable automation in knowledge sharing, and to facilitate the generation and refinement of this data. The research of Dandurand and Serrano (2013) defined eleven high level requirements that are necessary within CDXI, an overview of these requirements is provided in Table 3.2.

Table 3.2: High level requirements of CDXI (Dandurand & Serrano, 2013)

No.	Requirement
1	Provide an adaptable, scalable, secure and decentralized infrastructure based on a freely available code
2	Provide for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation
3	Securely store both shared and private data
4	Provide for customizable, controlled multilateral sharing
5	Enable the exchange of data across non-connected domains
6	Provide human and machine interfaces
7	Provide collaboration tools that enable burden sharing for the generation, refinement, and vetting of data
8	Provide customizable quality-control processes
9	Expose dissension to reach consensus
10	Support continuous availability of data
11	Enable commercial activities

In contrast with the digital knowledge sharing initiatives mentioned above are the Information and Analysis Centers, ISAC's, which are organized by the Dutch National Cyber Security Center (Nationaal Cyber Security Centrum, 2015). An ISAC is a public-private collaboration between organizations to improve their awareness and knowledge of cyber risks. Members of each ISAC will join in meeting between two and eight times a year to discuss occurred cyber incidents and possible solutions towards these threats.

3.2 Description of a risk

The second step within a risk analysis is describing the identified risks. The objective of such a description is to display the risks in a structured format (e.g. a table or a model) to identify the important structures and characteristics of the risk (IRM, 2002). ISRAM is a method to assess the probability and impact of an identified risk (Karabacak & Sogukpinar, 2005). Both the probability as the impact is described by factors that affect these elements. These factors will be translated into questionnaires that could be used to assess the risk, this estimation process will be described in more detail in Chapter 3.3. The risk rating methodology of OWASP uses the probability and impact of a risk as well, which are described by a fixed set of characteristics (OWASP, 2015a). The probability is divided between the threat agent and the vulnerabilities of the organization. The impact is based on the technical- and business impact, again will Chapter 3.3 provide more details on the risk estimation according to the OWASP Risk Rating Methodology.

An IT security risk should, next to the above mentioned probability and impact, describe at least the following three components: an overview of the system, an overview of the threat landscape, and the security properties (Bau & Mitchell, 2011). These three factors have an overlap with the above mentioned risk identification approaches: assets, threats, and vulnerabilities (NIST, 2012; Pfleeger et al., 2015). An overview of the system (or systems) that need to be secured should provide clear insights in the behavior of the system with intended as well as unintended operations. This overview could be based on existing documentation of the system that specifies the behavior. An overview of the threat landscape should be tailored to their possibilities of those threats. This could for instance be an overview of what the attackers can and cannot do when they have gained access to one of the organization's computers. The possibilities of the threat agents will usually depend on their computational resources (Bau & Mitchell, 2011) or its skill level and motivation (OWASP, 2015a). The security properties should define the ways in which threats are prevented or mitigated. The functionality of those properties should be validated with the possible threats to see if the systems are secure (Bau & Mitchell, 2011).

Another way to describe a risk is via the modeling of the events that lead towards, and result from the risk. These events could describe all of the, by Bau and Mitchell (2011) requested, elements (overview of the system, threat landscape, and security properties). These models are described in Chapter 4.3.

3.3 RISK ESTIMATION

The risk estimation step allows the analyst to further investigate the identified and described risks based on probability of occurring and potential impact. These estimations often result into a value for each risk to allow a prioritization between the risks. A risk value is often determined by multiplying the probability of the risk with the expected impact if the risk occurs (e.g. Fenton & Neil, 2013; Karabacak & Sogukpinar, 2005; NIST, 2012; OWASP, 2015a).

$$Risk\ value = Probability * Impact$$

Fenton and Neil (2013) proposed two limitations on this basic calculation of a risk value. At first there are multiple factors that determine the probability of a risk, it is therefore needed to further analyze the specific factors within a risk as well as the different approaches to determine the probability. The second limitation is caused by the fact that it is unclear what the risk value means, since this is dependent on the different approaches that determined the impact. Besides the two limitations Fenton and Neil mentioned that the power of a risk value is the ability to determine the impact of mitigations and controls on this value.

Several risk analysis methods are available that provide more detailed calculation to determine the individual probability and impact values. These approaches are described in Chapter 3.3.1 and 3.3.2, there are however methods to determine a risk value without these two values. These different risk estimation approaches are described in Chapter 3.3.3.

3.3.1 RISK PROBABILITY

Three general approaches to determine the probability of a certain event exist: Classical-, Frequentist-, and Subjective approach (Rausand, 2011). The classical approach is applicable in a limited set of situations. This approach requires a finite number of possible outcomes and the same chance for each possible outcome. Based on these preconditions it is possible to determine the probability of E with the formula below. This formula indicates that the number of favorable outcomes represents the number of outcomes in which event E is valid and the total number of possible outcomes represents all the events that are possible.

$$Classical\ probability\ measurement: P(E) = \frac{no.of\ favorable\ outcomes}{total\ no.of\ possible\ outcomes}$$

The frequentist approach is focused on phenomena that can be repeated under essential the same conditions. Each repetition is called an experiment and may or may not result into the event E (Rausand, 2011). The following formula is used to define the probability:

$$Frequentist\ probability\ measurement: P(E) = \frac{no.of\ events\ in\ which\ E\ occurs}{total\ no.of\ occured\ events}$$

The calculation of the probability of the event E is very similar as the classical approach. When there is enough historical data available this could be used to estimate the probability of a certain cyber risk (NIST, 2012). This approach however is not usable when there is not enough structured data available.

The last approach, subjective approach, determines the possibility of an event that cannot be determined by either the classical or the subjective approach. This approach represents an individual's degree of belief about whether or not an event will occur (Rausand, 2011). The probability of an event E, which is determined by an analyst with knowledge K will then be represented as:

$$Subjective\ probability\ measurement: P\ (E\ |K)$$

An advantage of the subjective approach over the classical- or frequentist approach is that it does not require a large amount of data. Due to the lack of structured historical cyber risk data (Byres & Lowe, 2004), several analysis methods are focused on some sort of subjective approach to estimate the risk probability.

Karabacak and Sogukpinar (2005) provide with the ISRAM method an approach to construct a structured survey that asks the opinion of employees from different departments of the organization to identify the state of different aspects that are relevant for a certain cyber risk. The questionnaire provides a weighted set of questions and answers that result into a general probability value of a certain risk. ISRAM does however not provide a fixed set of questions to identify the probability or impact of a certain risk, they only provide a structured approach to identify these factors, questions, and therefore the probability value.

A more structured approach to assess the probability value is provided by OWASP (2015a). They assess the probability on the vulnerabilities of an organization together with the threat agent that initiates the threat. The vulnerability is rated on the ease of discovery, ease of exploit, the awareness, and the intrusion detection and the threat agent is rated on its skill level, motive, opportunity, and the size (a single threat agent or a large group). All of the mentioned factors will be rated with numbered values (the values are translated to more relatable qualitative attributes) to calculate an average probability value that represents both the internal vulnerabilities and the threat agent's capabilities.

The risk assessment method as described by NIST (2012) suggests a combination between the use of the frequentist approach (by using historical data) together with information about the threat agent (comparable to OWASP (2015a)) and information about the organization's assets to better estimate the probability that a threat occurs and that it will lead towards a negative business impact. A factor that could influence the probability that a certain threat will lead towards a negative business impact is the speed of onset of a risk (COSO, 2012a). The speed of onset indicates the time it takes a certain threat to manifest itself into a certain business impact, where a high speed of onset indicates little time to control or mitigate the risk. This time is related to two other time events that could influence the business impact of a risk: time to compromise and the discovery time (Mcqueen, Boyer, Flynn, & Beitel, 2005; Verizon Enterprise, 2015).

The differences and overlap is displayed in Figure 3.1. It could however occur that the order of the events in Figure 3.1 is different, this could for instance be caused when the risk is earlier (or later) identified.

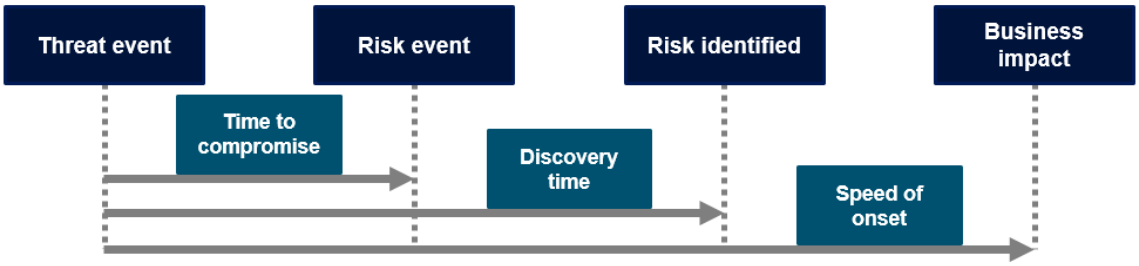

Figure 3.1: Time to compromise, discovery time, and speed of onset

The success of a cyber risk is, according to Byres and Lowe (2004), dependent on a function of three different variables. The first variable is a threat, which could be any event or circumstance with the potential to cause harm. Second, the presence of any vulnerabilities or weaknesses that could be exploited by an adversary. Last, the attractiveness of the target, where more valuable assets result into a more likely possibility to get attacked. These two factors fit into the Method-Opportunity-Motive framework of Pfleeger et al. (2015), which is in line with Routine Active Theory that reduces the opportunities of a threat agent (Choo, 2011). These three factors (a method, an opportunity, and a motive) are crucial for a malicious attacker to be successful (Pfleeger et al., 2015). Both the Method-Opportunity-Motive framework as the Routine Active theory indicate that a threat will not occur if one of those factors is omitted.

The above mentioned approaches are based on traditional criminal theories, these theories indicate that a crime can and will only occur if there is a suitable target in the presence of a motivated attacker and it is guarded by a weak defense (Cohen & Felson, 1979). These factors could be used to assess the plausibility of an attack, such as a cyber risk. An overview of these different theories and their categories is provided in Table 3.3.

Table 3.3: Needed factors for a successful criminal related activity

Criminal theory (Cohen & Felson, 1979)	**Successful cyber-attack estimation (Byres & Lowe, 2004)**	**Routine active theory** (Choo, 2011)	**Method-Opportunity-Motive framework (Pfleeger et al., 2015)**
Motivated attacker	Threat	Presence of opportunities	Method
Weak defense	Vulnerability	Absence of guardianship	Opportunity
Suitable target	Attractiveness of target	Motivation	Motive

3.3.2 RISK IMPACT

The risk impacts indicate the consequences if the risk actually occurs. An estimation of the financial damage often is used as a characteristic to determine the impact of a risk (Information Security Forum, 2015; OWASP, 2015a; Suh & Han, 2003). Suh and Han (2003) provide a more detailed calculation to quantify the costs of a cyber risk, which is in contrast with the more simplified cost estimation of OWASP (2015a) and the Information Security Forum (2015). The impact estimation method of Suh and Han (2003) determines the impact of a risk on the business model of an organization. This impact is based on the replacement costs of

damaged assets and the missed income due to a disruption of business processes or the unavailability of needed assets. The more simplified financial estimates are either a general, and unstructured, description of the financial impact (Information Security Forum, 2015) or a scale between five stages of financial impact (OWASP, 2015a).

Besides the financial impact results reputation damage, due to a cyber risk, into a large impact on a specific organization. Reputation damage could lead to the loss of clients or even permanently damage the brand of an organization (Choo, 2011). A disadvantage is the difficulty to quantify the actual (indirect) impact of the reputational damage. This problem is partly solved with the impact calculation by OWASP (2015a), they provide a scale to rank the reputation impact, this scale divides the impact between four categories: minimal damage, loss of major accounts, loss of goodwill, and brand damage. The overall business impact is calculated by taking an average between the above described financial and reputational influence together with their compliance towards regulations and possible privacy regulations (OWASP, 2015a). This average will result into a value between 0 and 9 to calculate the risk value and prioritize the risks.

Another impact calculation could be based on the technical impact. Although the business impact is considered to be more representable and reliable it often is more difficult to make an estimation of the business impact (OWASP, 2015a). The technical impact is aimed at the: loss of confidentiality, loss of integrity, loss of availability, and the loss of accountability. These factors are translated towards numeric values that allow the prioritization based on the impact of certain risks. The ISRAM method uses tailored factors, in contrast with the method of OWASP (2015a). The ISRAM factors result into a comparable overall impact value. This value is based, just like the probability estimation, on the answered questionnaires of the involved employees (Karabacak & Sogukpinar, 2005).

RISK APPETITE

The risk appetite indicates the amount of risk that is 'accepted' by the organization (ISACA, 2015). This value is the result of the strategic objectives of the organization. When an organization is pursuing strategic objectives it should be aware of, and accept, the underlying risk it is willing to undertake in doing so (COSO, 2012b). It therefore is important to develop, communicate, and monitor the risk appetite that is tailored to the organization's strategy. There is no 'standard' risk appetite that could apply to all the organizations (COSO, 2012b). Due to this fact it is needed for the organization to understand the trade-offs of having a higher or lower risk appetite. Factors that could determine the risk appetite include: the existing risk profile, the risk capacity, the risk tolerance, and the attitude towards the risk (COSO, 2012b).

3.3.3 DETERMINING A RISK VALUE

A lot of risk estimation approaches are based on the probability and impact of a risk as described in the beginning of Chapter 3.4. This value allows the prioritization of different risks, this prioritization is often visualized in a risk matrix (Rausand, 2011). Figure 3.2 provides a risk matrix that indicates the severity of a risk as proposed by OWASP (2015a). Based on the place of a risk in the risk matrix can be identified when a risk needs to be further evaluated.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Probability			

Figure 3.2: Risk matrix (OWASP, 2015a)

There are exceptions to the above mentioned calculation of a risk value. The Risk DREAD approach is one of the approaches that proposes a different approach (OWASP, 2015b). This approach determines the risk value on the possible damage, the reproducibility, the exploitability, the affected users, and the discoverability. This classification indicates a quantified estimate to compare and prioritize the amount of risk that is presented by a certain threat (OWASP, 2015b).

The approach by Suh and Han (2003) allows a risk calculation in monetary value by taking the recovery costs of the damaged assets as well as the loss of income due to unavailability of certain assets into account. The method calculates, as described above, the replacement costs of assets and the missed income due to the unavailability of certain assets. This calculation is based on the total business model of the organization and the part for which the affected assets are responsible.

The different approaches and methods that are described in the previous paragraphs could be divided between qualitative- and quantitative approaches. The differences between these approaches is comparable to the difference between a frequentist approach (quantitative, since it is based on data/information of events) and the subjective approach (qualitative, since it is based on the knowledge and experience of individuals). Table 3.4 provides an overview of the advantages and disadvantages of both of these approaches when assessing security risks (Pfleeger et al., 2015).

Table 3.4: Quantitative versus qualitative risk estimations (Pfleeger et al., 2015)

	Advantages	Disadvantage
Quantitative	- Results are based on objective processes and allow for meaningful statistical analyses. - Possible to express the value of assets and expected losses in monetary value, which is easier to understand. - Allows for a credible cost/benefit assessment of decision about controls.	- Risk calculations can be complex and therefor difficult to understand. - Needs a lot of information to perform the calculations. - Often there is no independently developed knowledge base to use with the analysis. Users must therefore rely on their internal knowledge base, or trust an external party.
Qualitative	- Calculation are often more simplified and easier understood. - Not needed to quantify the frequency and impact to exact values. - Not needed to estimate costs of mitigation measures for a cost/benefit analysis. - Provides a general indication of the most important risk areas that should be addressed.	- Results can be subjective and not independently. - Not possible to express objective costs and benefits of the risk analysis. - Difficult to track risk management performance in an objective manner (due to the subjective measures).

3.4 CONCLUSION

A general risk analysis consists of three steps: risk identification, risk description, and risk estimation. The identification of risks could be focused on the internal assets at risk, the known threats within the threat landscape, or at the vulnerabilities within the organization. According to Pfleeger et al. (2015) it is however needed to combine these three approaches to identify all the relevant risks. A way to complement the risk identification step, is risk related knowledge sharing. This allows an organization to use the by other organizations identified risks in their own analysis approach.

A risk should be properly described in order for it to be communicated with the various stakeholders. Descriptions vary from atomic risks or vulnerabilities towards more elaborate descriptions of the risk, its consequences, and potential indicators for that risk. Scenario based descriptions of risks will be further elaborated in the following chapter. The described risks are elaborated with risk values in the final step: risk estimation. These estimations are often based on the probability and impact of a risk and vary from qualitative estimations towards quantitative calculations. Both approaches have various advantages and disadvantages, it is therefore dependent on the context of the risk analysis which approach should be taken. An overview of the arguments for both qualitative and quantitative risk estimations is provided in Table 3.4.

4. RISK SCENARIOS

A lot of the risk analysis approaches (like the ones described in Chapter 3) are aimed at atomic risks, threats, or vulnerabilities. A risk scenario describes the events, as well as other relevant concepts, that cause and result from a certain risk. Creating such scenarios provides two main benefits (Roxburgh, 2009). First, one's thinking will be expanded, since he/she develops a range of possible outcomes. This range of outcomes is usually broader and more tailored to the specific situation than a pre-defined list of possible threats/risks. The second advantage is the ability to use the structure of events that cause the risk, to discover new ways to prevent or control such the negative consequences. These events are only identified once someone is forced to identify the complete risk scenario.

4.1 STORY OF A RISK

Roxburgh (2009) indicated that the story of a risk will only make sense if it provides the complete situation. A complete situation indicates that all the elements that have some relevance with the risk should be included in the story. The research of De Kock (2014) proposed a structure to capture all the relevant elements of risks related to terrorist behavior. An overview of the identified elements within the terrorist related stories is provided in Table 4.1.

Table 4.1: Elements to compose a story (De Kock, 2014)

Story elements	Description
Arena	Where did it take place?
Time (frame)	When the accident occurred and how long it took
Context	Additional details that are specific to this case
Protagonist	The victim within this case
Antagonist	The initiator (attacker) of the incident
Motivation	The reason the attacker initiated this incident
Primary objective	The desired goal of the attacker
Means	Any specific techniques or tools that were used
Modus operandi	Specific method of operation
Resistance	Difficulties that had to be overcome
Symbolism	A possible additional meaning of the act
Red herring	Any used decoys to complete the act

The proposed model was able to capture historic data in a structured manner to support law-enforcement agencies in the anticipation of terrorist behavior. An effective scenario model should satisfy three conditions (De Kock, 2014):

1. Offer the possibility to learn from historic criminal behavior.
2. Offer the possibility to adapt the chosen strategy on the basis of indicators that are found.
3. Offer the possibility to anticipate (unexpected) future real-world behavior.

Besides the above mentioned conditions such a model should provide guidance to identify all the relevant elements. A way to provide the entire situation is the use of the Golden W's, which are frequently referred to as: Who, What, When, Where, Why, in what Way, and With what (De Kock, 2014). The elements within the model of De Kock (2014) are therefore based on these W's.

4.2 Risk scenario concepts

A risk scenario consists, as indicated in the section above, of several different concepts. These concepts describe the different events that occur, as well as the other relevant contextual factors. This section describes several risk concepts, which are gathered from the NIST (2012) risk model, the OWASP risk rating methodology (OWASP, 2015a), and the CORAS security risk model (Lund et al., 2010).

Based on the above mentioned methods and models nine different concepts are identified to determine a risk scenario. These concepts, and their dependencies, are presented in Figure 4.1. Each of these concepts is further described below. The description of these concepts includes a cyber risk example of a phishing attack towards Company X.

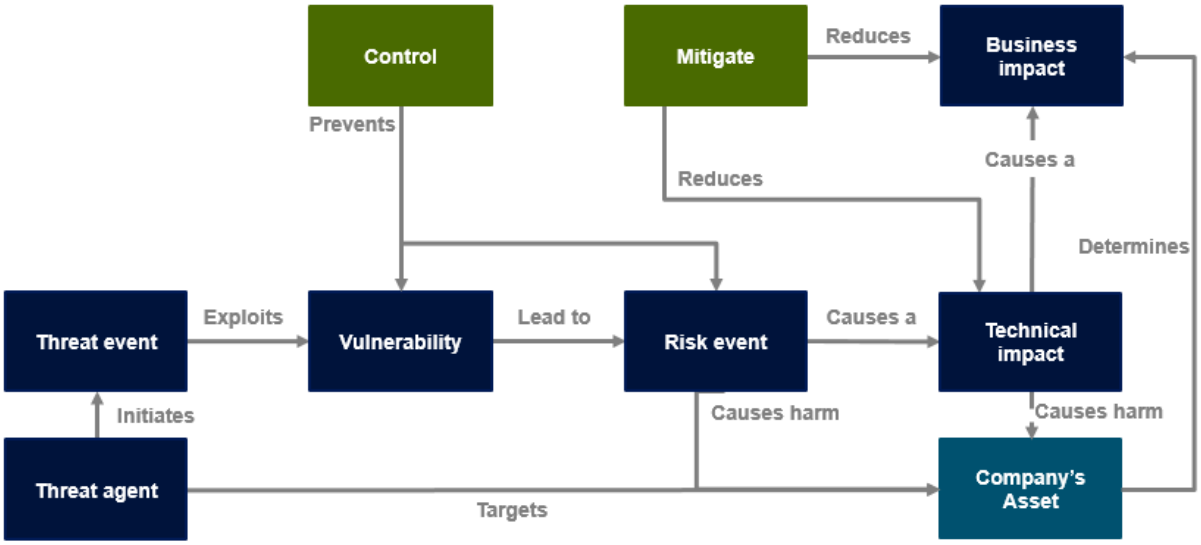

Figure 4.1: Concepts within a cyber risk scenario

Threat agent

A threat agent indicates an individual or a group that can manifest a threat to exploit certain vulnerabilities (OWASP, 2015a). Several types of threat agents, which have their own characteristics can be identified (Chapter 5.4 provides more information about these agents). In the case of the phishing example the threat agent is an individual cyber-criminal that targets the intellectual property of Company X via a phishing mail.

Threat event

A threat event, or trigger, is the first event in a risk scenario. This event can cause a certain undesired consequence if it is not controlled (Rausand, 2011). Fenton and Neil (2013) describe these events within the causal chain of the entire risk scenario. This chain could consist of several threat events that together results into a certain impact.

A human caused IT threat can be divided over malicious- or benign intent. Where the benign intent is caused by a human error the malicious intent is caused by an intended threat (Lund et al., 2010; Pfleeger et al., 2015). Another distinction between directed, and random threats can be made. A random threat can be malicious code which is spread through a general website, a directed threat is the result of a more specific and intended attack (Pfleeger et al., 2015). Figure 4.2 visualizes the structure of these different threats.

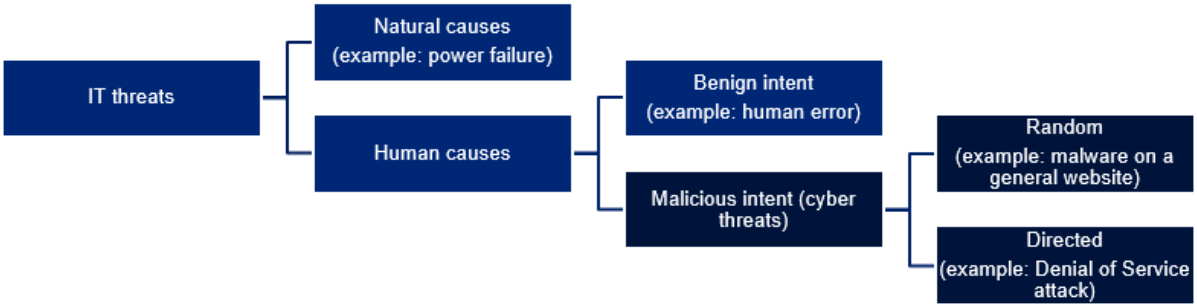

Figure 4.2: Different kind of IT threats (Pfleeger et al., 2015)

Regarding the phishing example two important threat events can be identified. The first threat event is the phishing mail that has been sent by the above mentioned threat agent. The second threat event is an unaware employee that opens the attachments of this email.

Vulnerability

A vulnerability is a weakness of a specific information system, security procedure, or internal controls that can be exploited by a threat agent. These vulnerabilities often are broader than the information system and could include the organizational governance structure, external relationships, or the information systems security architecture (NIST, 2012).

Due to the fact that the organization's employees are possible vulnerabilities it is difficult to protect all the vulnerabilities with technical solutions. Awareness and education or training therefore should be part of an effective protection of the vulnerabilities (Choo, 2011).

A vulnerability in the phishing example is the awareness, or more the lack of awareness of the employee for phishing mails. If the employee would have been more aware of such threats, he would not have opened the attachment and thereby prevented any caused business impact. With a deeper analysis of the situation it will be possible to identify several vulnerabilities (e.g. a better spam filter for phishing mails or a better virus scanner to check the downloaded email attachments).

Risk event

The event that causes the impact in a risk scenario is the risk event itself. In the case of a phishing mail the risk event is that a hacker can, due to the malicious software that he provided in the phishing mail, enter the software system. It can be difficult to determine the difference between cyber threat events, and a cyber risk event, this is due to the fact that the above provided distinction is based on the order of the threat events.

TECHNICAL- AND BUSINESS IMPACT

Cyber risks can cause different kinds of impact. A distinction between a business- and a technical impact can be made (OWASP, 2015a). The business impact is focused on financial or reputation damage, and the technical impact on the implications of the cyber risk on the (software) systems.

The technical impact within the phishing example is the fact that the software system is breached. This indicates that the hacker who sent the original phishing mail can now enter the systems, and of course depending on the security of the system, access the various data assets of Company X. To indicate the importance and a more tangible implication of a cyber risk it is important to define the business impact of the risk. The business impact of the phishing example can be that the intellectual property (IP) is stolen. This can however be further defined to an even more concrete business impact which is the loss of competitive advantage. The implications of such a business impact can vary a lot per organization, for instance the IP is more important for a production organization than an online retailer (Chapter 5.3 provides more information about the possible impact of a cyber risk).

RISK CONTROLS AND MITIGATIONS

A control is applied to prevent the risk to occur, and a mitigation is applied to reduce the impact of an occurred risk (Fenton & Neil, 2013). The controls and mitigations can be applied on all the events within the risk scenario. In the phishing mail example there are both controls and mitigations possible. A possible control is an awareness training towards the threats of a phishing mail, which aims to prevent these kind of risks to occur. A mitigation could be applying multiple security levels within the software system. This will limit the amount of access that the cyber-criminal has after his successful phishing attempt, and therefore mitigate the business impact.

ASSET

An asset is something that is targeted by the threat agents and therefore needs to be protected by the organization (Lund et al., 2010). An asset can for instance be the intellectual property, or privacy sensitive information of an organization. Besides the data examples an asset can be the trust of the customers or the availability of a server.

The asset that is targeted by the threat agent, in the phishing mail example, is the intellectual property of Company X. Another asset that could, without the intent of the threat agent, be harmed is the trust of the customers of Company X.

A COMPLETE RISK SCENARIO

The above mentioned concepts can be formed into a risk scenario. This will provide an overview of the different events that together will cause the business impact. Figure 4.3 provides an overview of the structure of these events. The structure of this scenario differs with Figure 4.1 since there are two threat, and business impact events captured in the scenario.

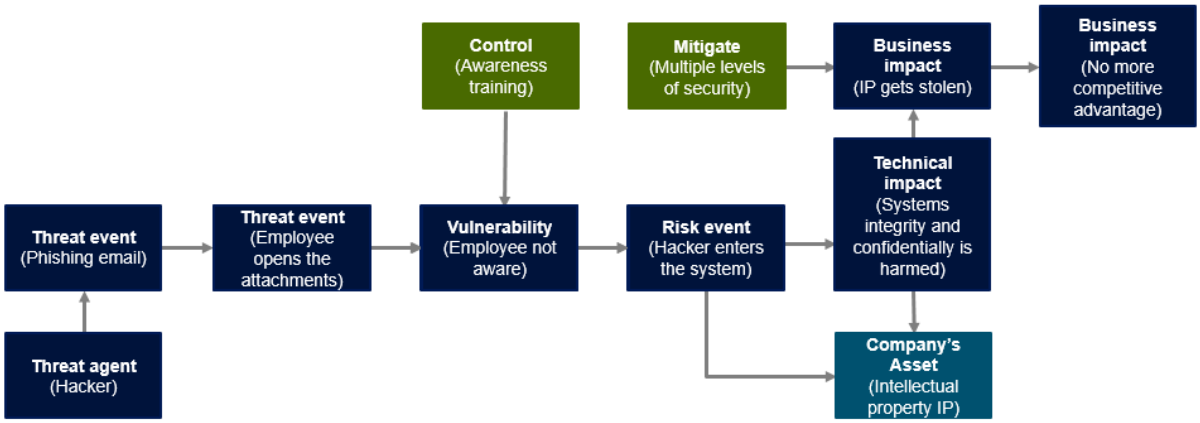

Figure 4.3: Cyber risk scenario of a successful phishing attempt

4.3 CAUSAL MODELING TECHNIQUES

As indicated by Roxburgh (2009) in the beginning of this chapter it is needed to identify all the relevant elements within the story of a risk. These elements could be captured within a causal model to capture the dependencies between the contextual elements and the causal structure of the threat events in a risk scenario. A causal model to capture these elements should at least consist of the following elements (Fenton & Neil, 2013):

- The event itself (the risk)
- One or more consequence events that represents the impact of the risk
- One or more trigger, or initiating, events
- One or more control events that may stop the trigger event(s)
- One or more mitigating events that reduce the impact of a negative consequence

An example of a causal chain that contains all of these elements is provided in Figure 4.4.

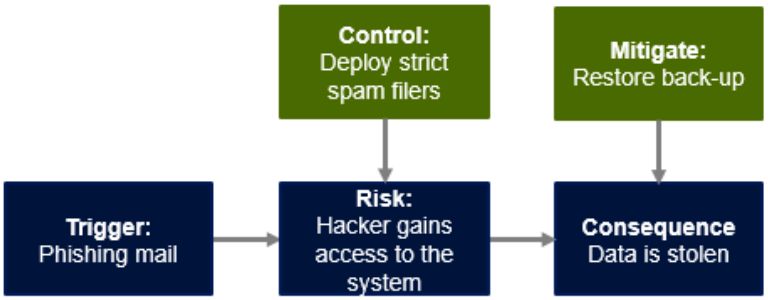

Figure 4.4: Possible causal chain of the risk of a stolen data due to a phishing mail

The risk scenario created in Figure 4.3 (in Chapter 4.2) can be seen as an elaborated version of the by Fenton and Neil (2013) defined causal model, which is displayed in Figure 4.4. Besides the general causal chain

provided in Figure 4.4 are several techniques to guide the modeling of causal chains. Rausand (2011) identified the following techniques: cause and effect diagram, fault tree analysis, Bayesian networks, Markov methods, and Petri nets. A limitation to the cause and effect diagram is that it is not possible to provide quantitative answers, it merely shows the causal structure of the investigated events (Rausand, 2011). For that reason, the cause and effect diagrams are not described in this section. The Markov method is omitted as well, this is due to the fact that Petri nets could be seen as a replacement for that method (Rausand, 2011).

The above mentioned list of Rausand (2011) is extended with the following models: a bow-tie model to extend the fault tree analysis (Fenton & Neil, 2013; Rausand, 2011), an Influence diagram (as described by Howard and Matheson (2005)), the CORAS model (Lund et al., 2010), and the ANRAM model (Bex & Hovestad, 2016; Bex, 2011), which is based on the Hybrid theory Bex (2011).

4.3.1 BOW-TIE MODEL

A bow-tie model provides an overview of the different events that together cause the risk event, as well as the different consequences resulting from the risk. These chains of events include the barriers that have been implemented to prevent the risk from occurring, or mitigate the consequences (Rausand, 2011). The events that lead towards the risk is modeled as a fault tree, where the consequences of the risk are modeled as an event tree (Fenton & Neil, 2013).

A fault tree analysis is suitable for qualitative as well as quantitative analysis of complex systems. The model displays the different events that have a certain impact on the risk event. Although a fault tree is usable for the analysis of complex systems it is difficult to maintain, and therefore it is less useful for the analysis of a dynamic environment (Rausand, 2011). An event tree displays the possible accident scenarios that result from a specific risk scenario. The probability values are modeled within the event tree to provide a better overview of the chances of each scenario (Rausand, 2011).

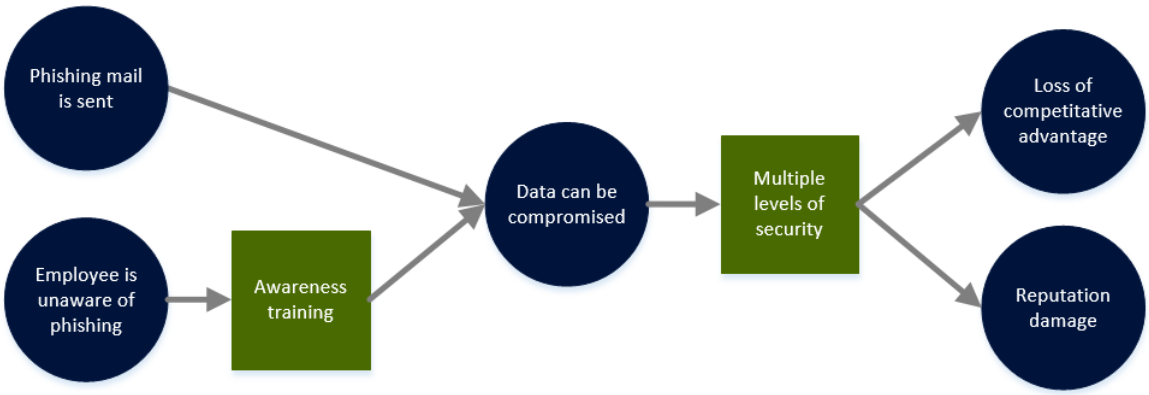

Figure 4.5: Bow-tie diagram of the risk of a phishing mail

A bow-tie model can be visualized in various ways. Figure 4.5 provides an example of a (simplified) bow-tie model of a phishing mail example. A more complex bow-tie could include a hierarchical structure of the triggers and/or the consequences of the risk. Within the figure are threat-, risk-, and consequence events displayed as blue circles and the controls and mitigations as the boxes.

4.3.2 CORAS

CORAS consists of both a model and a method to identify, evaluate, and control security risks. The results of the method are captured in a modeled risk scenario, and one or more treatment scenarios. These models are built with relatable icons to easily communicate the threats in the model (Braber et al., 2007). Estimation and evaluation steps are included to estimate the likelihood (or probability) and as the impact of the risk.

The likelihood and impact estimations are identified during workshop sessions. The participants of the workshop together estimate the values, based on their experience and knowledge. For more complex risk scenario that are difficult to estimate could the 'analysis leader' (the lead during the workshop session) provide historical data or personal experience about comparable threats (Braber et al., 2007). The impact estimations are determined within five qualitative stages between insignificant towards catastrophic, the likelihood estimations are categorized in five qualitative categories as well (between rare and certain). Based on these two values is determined if a risk needs to be treated. Such a treatment can be visualized with treatment scenarios that describe a treatment to control or mitigate a certain threat scenario or unwanted incident. These scenarios are modeled with a fixed set of icons and could be combined to display the threat of a phishing mail (as displayed in Figure 4.6). Within the model in Figure 4.6 it is possible to apply treatment scenarios to the vulnerability as well as the threat scenario and unwanted incident.

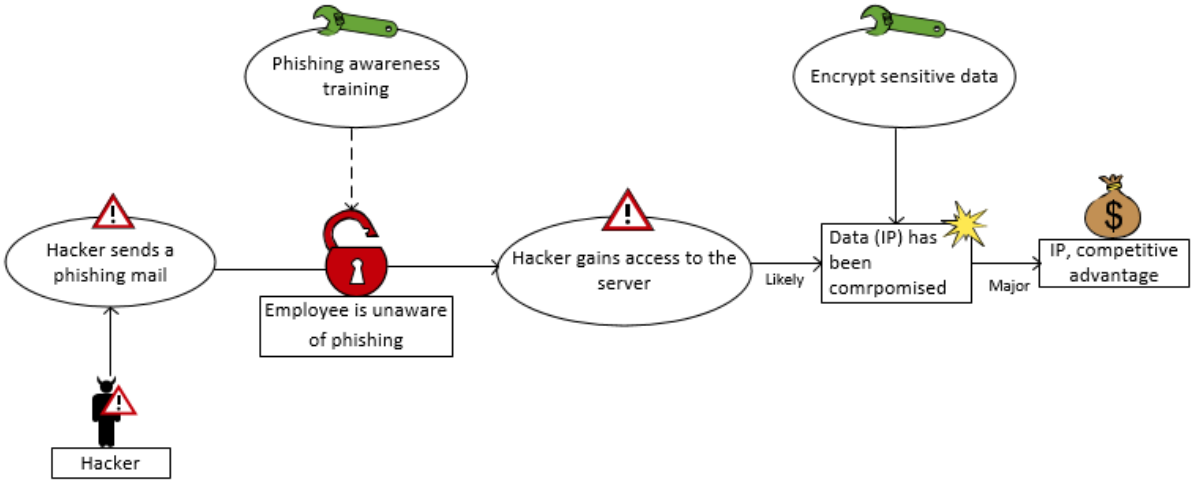

Figure 4.6: CORAS model of the risk of a phishing mail

4.3.3 INFLUENCE DIAGRAMS

An Influence diagram can be used to model the flow of information or events as well as the probabilistic dependencies (Shachter, 1986). This model is constructed with decision nodes (represented by boxes) and chance nodes (represented by circles) (Howard & Matheson, 2005). These nodes are connected via informational- or conditional influences. The informational influence lead towards a decision node and represents the variables that will be known when the decision is made (Howard & Matheson, 2005).

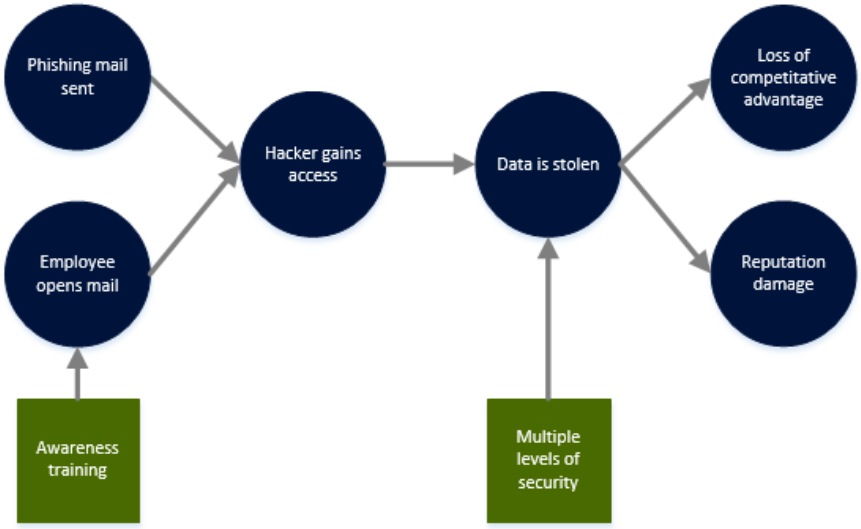

Figure 4.7: Influence diagram of the risk of a phishing mail

Figure 4.7 displays the threat scenario of a phishing mail within an Influence diagram. An Influence diagram can, besides the visual representation, be used to calculate and express the probability values between the different nodes. An advantage of influence diagrams is the possibility to quantify these probability values to perform a quantified analysis as well.

4.3.4 BAYESIAN NETWORKS

A Bayesian network represents several nodes that are connected with a probabilistic dependency (Vlek, Prakken, Renooij, & Verheij, 2013). The dependencies between the nodes are visualized by the arrows in the network. Figure 4.8 provides a Bayesian network of the phishing example. Next to the dependencies between the nodes are the probabilities of each of these nodes, given their parent nodes, visualized (note: the probability percentages in Figure 4.8 are not representative). These probability values in a Bayesian network provides an overview of the quantified 'chance' that a certain risk occurs. This overview is provided by the Node Probability Tables (NPTs) in the graph. The nodes within the Bayesian network displayed in Figure 4.8 only consist of a 'true' or 'false' probability, it is possible to tailor these options when needed (e.g. a category or a scale).

The NPTs in the network provide the probability distribution of a node given the probability distribution of his parents. A properly modeled Bayesian network adjusts the probability distributions of a node if the distributions of his parents is changed. This functionality is useful to visualize the effect of (applied) controls or mitigations on the risk consequences. In Figure 4.8 is an awareness training as a possible control implemented, this control is however not active (the scenario is modeled as: false). When this awareness training is in place, it will affect the remainder of the network.

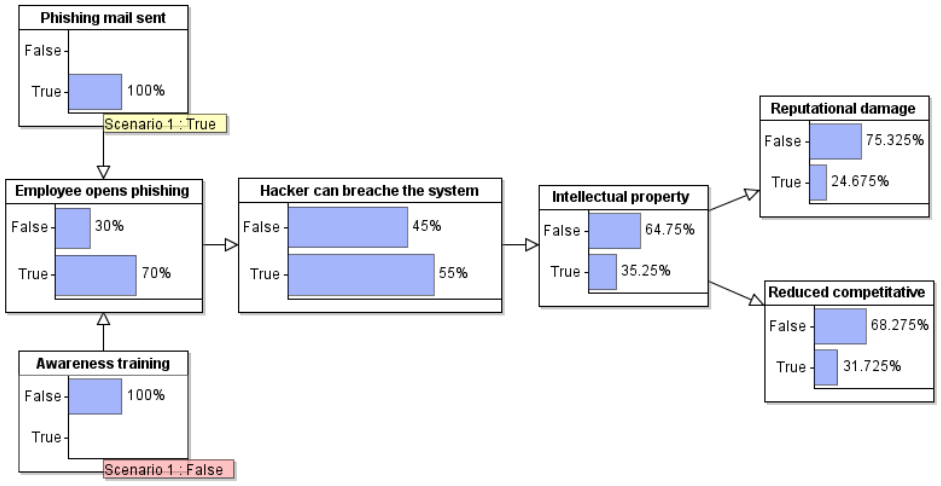

Figure 4.8: Bayesian network of a phishing attempt without awareness training

There are several software tools available that help with the creation of a Bayesian network (the example in Figure 4.8 is created with software of AgenaRisk (2016)). The process to create this network consists of the following steps:

1. Identify the set of variables that are relevant in the specific situation
2. Create nodes for all the identified variables
3. Identify the direct dependencies between the different nodes
4. Identify qualitative dependencies in the graph
5. Specify the NPT for each node in the graph

4.3.5 ANRAM

ANRAM is a risk model that is based on the Hybrid theory (Bex & Hovestad, 2016). The Hybrid theory consists of a combination of two different approaches to sense-making: the story-based approach and the argument-based approach (Bex, 2011). The combination between these approaches could be applied to reason about evidence in order to determine the certainty of facts in a case (Bex & Hovestad, 2016; Bex, 2011). This approach, which is based on formal and informal reasoning, is suited to perform an analysis of individual pieces of evidence within a certain scenario, and is suited to perform a causal analysis of the different events in the scenario, and could be performed with ANRAM (Argumentative-Narrative Risk Assessment Model). The argumentative approach allows reasoning about the certainty of each of these events. This reasoning is based on different pieces of evidence. Figure 4.9 provides an overview of a phishing attempt, modeled in ANRAM. The purple boxes in the model display pieces of evidence that affect claims (grey boxes) or risk events (orange boxes) in the scenario, such evidence can support or weaken a claim. When the box is connected with an arrowhead it will support the claim, a square instead of the arrowhead indicates that the claim is attacked by an additional piece of evidence. The green box in the model, which is currently not connected within the causal structure, displays a possible control to prevent or mitigate a threat from occurring. Besides the causal structure it is possible to model the dependencies between events with different connectors. These include an AND connector, an OR connector, and a XOR connector.

An advantage of this approach is the combination between the story of the risk with the argumentation to prove this story. This is in contrast with existing approaches to reason with evidence that are either story-

or argument-based (Bex, Koppen, Prakken, & Verheij, 2010). In the case of a cyber risk it is possible to model the causal structure of a risk and provide evidence that support certain claims within this story.

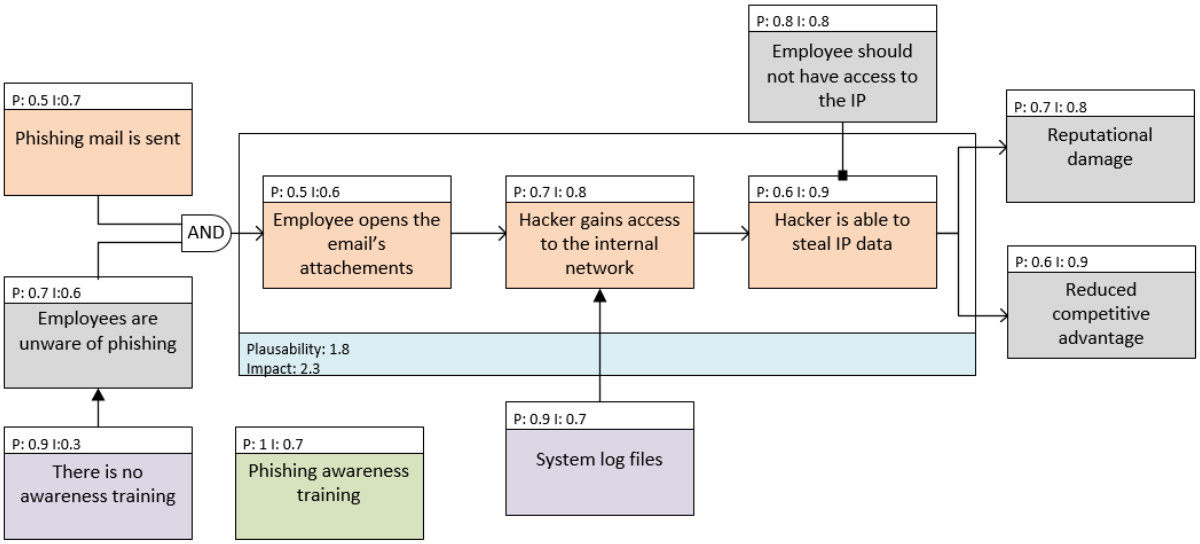

Figure 4.9: A phishing attempt

This model provides, as displayed in Figure 4.9, both the story of the risk event as arguments to support or attack the trustworthy of the described events. These events could be described within a scenario to represent the overall plausibility and impact. The values of each argument are ranked between 0 and 1. The scenario's overall plausibility and impact is, based on the different arguments, determined. A risk scenario, within ANRAM, consist of the central risk event, the direct actions that are connected to this event, relevant risk factors, possible controls, other relevant information, and a pattern of actions which shows how the events are connected (Bex & Hovestad, 2016).

4.3.6 PETRI NETS

Petri nets can be used to express the causal structure of several events. These events are divided over states (circles) and transitions (rectangles). In the example Petri net, Figure 4.10, a possible sequence of events of a phishing attempt is modeled. An advantage of Petri nets is the possible quantitative analysis, which is possible due to the dynamic behavior in the model. This behavior is expressed by 'tokens' that travel over states via the transitions. These simulation possibilities make Petri nets perfect for the analysis of complex processes or risk events (Rausand, 2011).

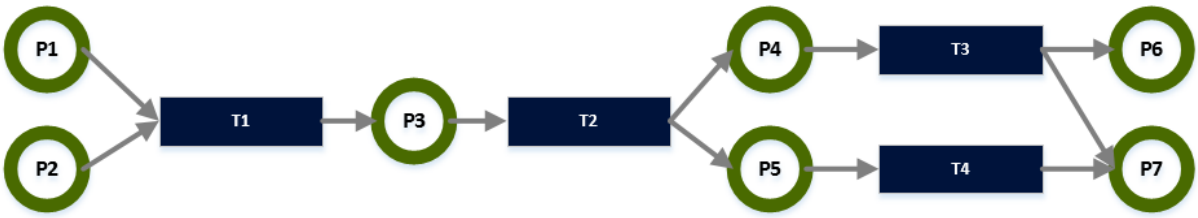

Figure 4.10: Petri net of a phishing attempt

The example Petri net in Figure 4.10 displays eight different states which are connected via four transitions. The first two states (P1 and P2) are that a phishing mail is send, and that an employee opens the malicious attachments of this phishing mail. The first transition (T1) could result into P3 if both P1 and P2 are considered true. P3 is the main risk event in this example: the hacker gets access to the organization's system. The second transition could trigger two new states, P4 which indicates that the hacker steals confidential data, and P5 that indicates that the hacker shuts down crucial systems. As indicated in the model both of these events will result into P7: reputational damage, and the stolen data will result into a loss of competitive advantage as well.

4.4 CONCLUSION

Risks should not only be seen as atomic events or elements that causes a negative impact. Risks are often better explained as a combination of events that together cause that negative impact. The combination of these events can be seen as a risk scenario. Such a scenario provides more valuable context about the risk itself since it describes the entire story behind the risk. Especially in the case of cyber threat, which can be seen as the IT threats that have a human cause and a benign intent, it is important to look at the entire story. Another advantage of a scenario based risk assessment is the needed combination between a threat-, an asset-, and a vulnerability based approach (Pfleeger et al., 2015). This combination is identified since the scenario describes several threat events that are targeted to an asset, and could occur due to one or more vulnerabilities.

The study towards risks scenarios identified the nine different concepts that should be present within a human intended risk scenario. This is needed since a cyber risk can be seen as a human, with malicious intent, caused IT risk. The identified elements are as follows: a threat agent, one or more threat events, vulnerabilities, a risk event, a technical- and a business impact, risk- controls and mitigations, and an asset that is targeted by the threat agent. A combination of these concepts could construct a cyber risk scenario.

The last section of this chapter described causal models which can be used to capture risk scenarios and to estimate probability and/or impact values. These models vary from quantitative/mathematic models (such as Bayesian network), towards more qualitative models (such as the CORAS method). As described in Table 3.3 in Chapter 3.3.3 there are advantages and disadvantages for both the quantitative and qualitative estimation approaches. It is therefore important to alter the choice of these models towards the needs of the specific situation.

5. CYBERSPACE

This chapter provides more insights in the topics that are related with cyberspace. Cyberspace can be defined as the complete environment in which communication over computer networks occurs (Bell, 2004). This environment includes all the information- and non-information-based assets that are stored, transmitted, or vulnerable via IT (Solms & Niekerk, 2013). The organization's products, employees and its customers therefore are, next to the information based assets, vulnerable to cyber threats.

As mentioned in the problem statement (Chapter 1.1) a clear understanding of the threat landscape is needed to make informed decisions about the mitigation- and controlling of risks (Choo, 2011). This chapter provides a better overview of the overall cyber threat landscape by describing the recent developments within this landscape. Besides these recent developments the different categories of cyber threats are described, this is followed by a description of the different impact of those threats towards different organizations/industries and a description of the different threat agents that are active within the cyber threat landscape. The remainder of this chapter will focus on the practices to become resilient towards cyber threats.

5.1 THE CYBER THREAT LANDSCAPE

A cyber threat landscape indicates all the threats and risks towards an organization, industry, country, or even the world that can occur in the context of cyberspace. A study towards the development of the global cyber threat landscape between 1980 and 2009 is conducted by Beggs (2010)**.** This study identified a growing sophistication of cyber threats over the years, which is in line with a study of ENISA (2013), who identified a growth in available sophisticated tools to perform a cyber risk. The growth in sophistication is confirmed by Verizon Enterprise (2015), who provided an overview of the developments between 2010 and 2014. Their overview was focused on the biggest changes in the cyber threat landscape and identified that the use of sophisticated attacks as spear phishing and RAM scraping has grown but the use of simple spyware (like key loggers) and credential guessing has decreased.

More recent studies provide comparable results. One of the most influential development is caused by the Internet of Things (IoT). The IoT indicates all the devices that are connected with the internet. The total amount of internet-connected devices is expected to rise from 1.2 billion in 2014 towards 5.4 billion devices in 2020 (Verizon Enterprise, 2015). Attacks that are based on the IoT will therefore become mainstream risks (Sophos, 2015; Verizon Enterprise, 2015). The number of threats in the threat landscape is growing as well (Information Security Forum, 2015), this is due to the fact that IoT devices have often failed to implement basic, and necessary, security standards (Sophos, 2015). A side note to the growing threats accompanied with the IoT is the fact that mobile devices do not seem to be preferred vectors in data breaches via malicious code, only 0.03% of a tested group of millions of devices was infected with malicious code to exploit a data breach (Verizon Enterprise, 2015).

Another development in the current threat landscape is the growing regulatory influence of governments. This can be identified by the regulations towards disruptive organizations, such as Uber, Airbnb, and Google

(Information Security Forum, 2015), as well as the stricter national and international regulations regarding privacy and data security (Sophos, 2015).

An estimation of the cost of cyber risk related activities to the global economy is performed by McAfee (2014), their estimation indicated that this costs would be over 400 billion USD (Choo, 2007). This amount is comparable with other criminal activities such as illegal drugs sales or counterfeiting (McAfee, 2014), and due to the predicted growth of E-commerce in the coming years the cyber-crime opportunities will grow as well (Information Security Forum, 2015).

5.2 CYBER THREATS

Cyber threats include, as explained in Chapter 4.2, all the threats that are related to the IT landscape, and are caused by a benign human intent. The growing sophistication of the cyber threats within the landscape together with the complex IT infrastructure of organizations has resulted in a large amount of cyber threats (Pfleeger et al., 2015). This large amount of different threats could be classified into three general categories: unauthorized computer and data access, deployment of malicious software, and disruption of business processes (Clough, 2010). A challenge within the categorization of cyber threats is the possible overlap of threats between these categories, as well as the rapid and continuously changing threat landscape. A more general division that could be made is between advanced persistent threats (APTs) and 'normal' threats. An APT can be defined as a sophisticated multi staged attack by an attacker with expertise and significant resources (ISACA, 2015).

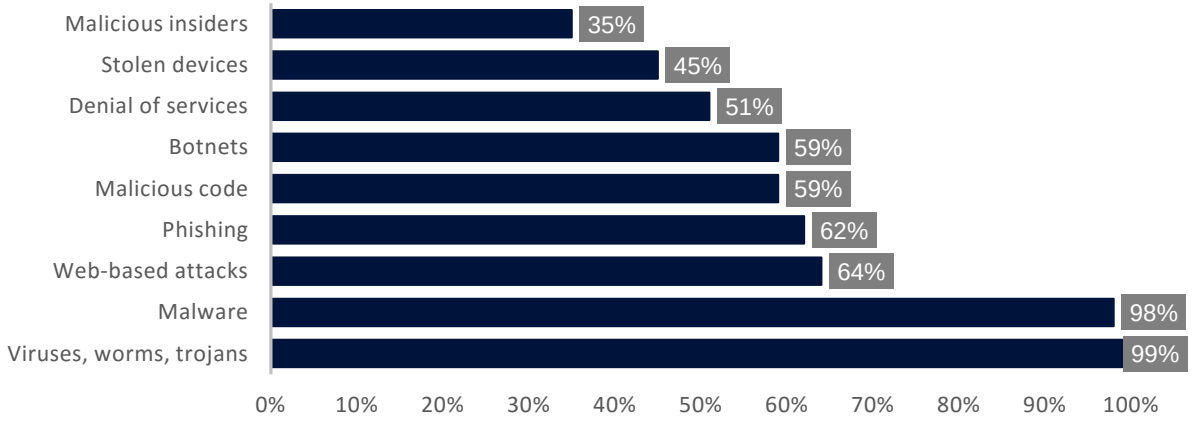

Figure 5.1: Most occurring cyber threats (Ponemon Institute, 2015)

A survey of the Ponemon Institute (2015) resulted in the nine most occurring cyber risks. The survey was conducted at 252 organizations in 7 countries (USA, Germany, Japan, United Kingdom, Brazil, Australia, and Russia). Figure 5.1 provides an overview of these nine most occurring cyber threats in the surveyed organizations. The horizontal bar indicates the percentage of the surveyed organizations that were harmed by such a threat. The remainder of this paragraph will discuss these cyber risks in more details within the categorization by Clough (2010).

5.2.1 UNAUTHORIZED COMPUTER ACCESS

Unauthorized access is obtained when someone uses a computer without permission. This access could be achieved in a physical and a digital way. Three motivations are identified to gain unauthorized access to a

computer system: access and gather to data or information, make use of the computing power, and modify existing data (Clough, 2010).

DATA GATHERING

The value of the large amount of information that is stored on computers and in computer networks, is an obvious motivation for gaining access to those computers and systems. The information includes confidential commercial and/or government information (e.g. trade secrets, intellectual property, defense secrets) or personal information (e.g. medical records, credit card or social security numbers or credit history). A significant amount of the cyber risks are aimed at the illegal gathering of data (Clough, 2010).

Phishing, which has occurred in 62% of the surveyed organizations, is a form of a semantic cyber risk. The aim of a semantic cyber risk, is to seek for social vulnerabilities (Choo, 2011). A phishing mail is a message that purport to originate from legitimate organizations (e.g. banks and financial services) to deceive victims to provide information or to deploy malicious software (Choo, 2011; Pfleeger et al., 2015). The effectiveness of those phishing mails is investigated by Verizon Enterprise (2015). Their study indicates that on average 23% of the recipients of phishing mails will open the message, and 11% open the attachments.

A web-based attack aims to breach a certain IT system via the internet (SANS Institute, 2007). This attack is focused on breaching the application layer behind the network of a certain organization. This layer will provide access to valuable information such as the intellectual property of a product, or privacy sensitive information of its employees or customers. According to the Ponemon Institute (2015) 64% of the organizations have experienced a web-bas attack.

Physical oriented risks that are related to illegal gathering of data are theft of corporate devices or the risk of a malicious insider. Such a device often contains a lot of sensitive and valuable information, which could be more valuable than the hardware itself (Ponemon Institute, 2015). The malicious insiders as indicated by the Ponemon Institute (2015) results into the ninth most common cyber threat. The reasons that these insiders act as a threat agent vary, it could be because of dissatisfaction, frustration, or due to some sort of corruption (ENISA, 2013). Chapter 5.4 will provide more insights in the different threat agents and includes malicious insiders.

USE OF A COMPUTING POWER

The severity of the cases in which computing power is misused varies a lot. A form of misuse could be that an employee is using his work computer for non-work purposes (Clough, 2010). A more severe misuse is the application of botnets. Botnets allow the attackers to remotely control other computers once they have turned these computer into so called ‘zombies’ (Choo, 2007). A botnet connects these ‘zombies’ to controlling computers, these controlling computers are now capable to send commands to the ‘zombies’ (Choo, 2007).

MODIFICATION OF DATA

The last motivation to gain unauthorized access to a computer or system is the ability to modify data. A threat agent could for instance delete or modify data so that it will become worthless or misleading. Other motivations include the gain of financial benefit by for example increasing a line of credit or the need to conceal your ‘digital’ presence by modifying the system logs after you have breached a certain system (Clough, 2010).

5.2.2 DEPLOYMENT OF MALICIOUS SOFTWARE

The second cyber risk category is the deployment of malicious software. Malicious software can be defined as any piece of software with bad intentions (Clough, 2010). The definition of malicious software based on the intent distinguishes this threat with the risk of unintentional errors or minor flaws within good intended software. (Pfleeger et al., 2015)

Although the Ponemon Institute (2015) provides loose categories for viruses, worms, and Trojans all of these software pieces can be defined as malicious software (malware). This malware affects a large amount of organizations (99 percent), a smaller amount of the organizations was affected by a malicious code attack (59 percent). The differentiation between malware and malicious code is in this case the fact that malicious code attacks are malware attacks that have successfully infiltrated the organizations' networks and/or systems (Ponemon Institute, 2015).

Pfleeger et al. (2015) defined a virus as a malicious piece of code with a specific purpose that has an intent to spread itself. This is comparable with a computer worm, which is a malicious piece of code that spreads copies of itself as well. The difference lies in the fact that a computer worm does not need a human action to spread where a virus does. A Trojan horse is a software program that has a benign apparent, but a hidden malicious effect. A Trojan horse does however not replicate itself (Pfleeger et al., 2015).

Choo (2011) identified a difference between generic- and customized malware. Where general malware is spread via website without a specific target is customized malware tailored towards a specific target. The use of this customized (and often more sophisticated) malware has grown in the recent years. This customization is partly caused by the introduction of malware toolkits (Choo, 2011). Malware toolkits allow the development of sophisticated malware without programming knowledge and skills.

5.2.3 DISRUPTION OF SERVICE ATTACK

The disruption of the business processes could be caused by the malfunction of software systems due to malware (as described in Chapter 5.2.2) or via a Denial of Service (DoS) attack. The research of the Ponemon Institute (2015) revealed that 51% of the investigated organizations has been affected by some sort of DoS attack. A DoS attack attempts to disable the availability of a system or entire network (Pfleeger et al., 2015).

A DoS attack can be achieved at various ways. A network router could be disabled or reprogrammed in order to disable all the access to the network or the network could be overwhelmed via a large amount of mails or a replicating virus that are (automatically) send towards the organization (Pfleeger et al., 2015). A threat agent could use botnets (as explained above) to overwhelm the network from several computers at once. Such a distributed attack is called a DDoS attack (Distributed Denial of Service).

5.2.4 OTHER CYBER RISK CATEGORIZATIONS

Besides the cyber risk categorization of Clough (2010), several other categorizations exist. These categories vary in detail and their focus. Where some categories are focused towards the goal of a threat event (e.g. IRAM2) are others focused towards the different stage within a cyber risk (the cyber kill chain). The different categorizations are described below.

STEPS WITHIN A CYBER RISK

The process of a cyber risk can be described as a kill chain (Lockheed Martin Corporation, 2015). This kill chain consists of seven consecutive steps that a threat agent needs to follow if he wants to conduct a successful attack. According to Lockheed Martin Corporation an attacker will only succeed if he successfully

reaches the last stage of the chain. This provides the opportunity to stop a possible cyber risk in six different ways. The seven steps of the chain are displayed in Figure 5.2.

Figure 5.2: The cyber kill chain (Lockheed Martin Corporation, 2015)

The steps of the kill chain describe the preparation phase of the attacker (step 1 until 3), and the following steps that are executed to achieve the specific goal of this attack. The steps describe the use of exploits and malware to gain access to a specific computer system to cause a certain cyber risk. The actual risk and possible impact is not in scope of this chain.

The Lockheed Martin Corporation (2015) identified multiple ways in which the kill chain could be applied. The kill chain can, at first, be used to prioritize actions resulting from sensor alerts. The position of the resulting event on the kill chain will determine the priority. Other advantages of the kill chain include the ability to prioritize your security investments and measure its effectiveness. This is possible since each stage has its own approaches to detect and deny the actions of the attacker. Regarding effectiveness: it is desirable to stop the attacker as early in the kill chain as possible.

STRIDE-LM

STRIDE is a threat based classification schema for the characterization of cyber threats. The classification was originally created by Microsoft (Microsoft, 2005; OWASP, 2015b), and expanded by the Lockheed Martin Corporation to the STRIDE-LM categorization (Muckin & Fitch, 2015)**.** The acronym STRIDE-LM stands for: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege, and at last lateral movement. The research of Muckin and Fitch (2015), commissioned by the Lockheed Martin Corporation, resulted in an overview of the targeted properties and possible controls for each of the categories of STRIDE-LM.

ISF IRAM 2

The Information Security Forum created a general overview of the different types of cyber threats, and mapped this overview with possible controls within the IRAM2 framework (Information Security Forum, 2014). Their framework identifies 22 different threat events within 12 threat types. For each threat event there are prioritized controls, and a sophistication level provided. The different threat events, and their sophistication, is provided in Appendix A.

CAPEC'S ATTACK PATTERN REPOSITORY

The MITRE Corporation (2015) deployed a repository that contains over 500 different cyber-attack patterns. These patterns are divided over several categorizations to provide a better overview of the different patterns, the first division is made between attack- domains and mechanisms. The different domains are: social engineering, supply chain, communications, software, physical security, and hardware. These domains are further specified into the different attack patterns.

5.3 IMPACT OF A CYBER ATTACK

The Ponemon Institute (2015) identified the four highest cost components that resulted from cyber risks. These four categories are: business disruption, information loss, revenue loss, and equipment damage. The relative influence of each of these components is displayed in Figure 5.3.

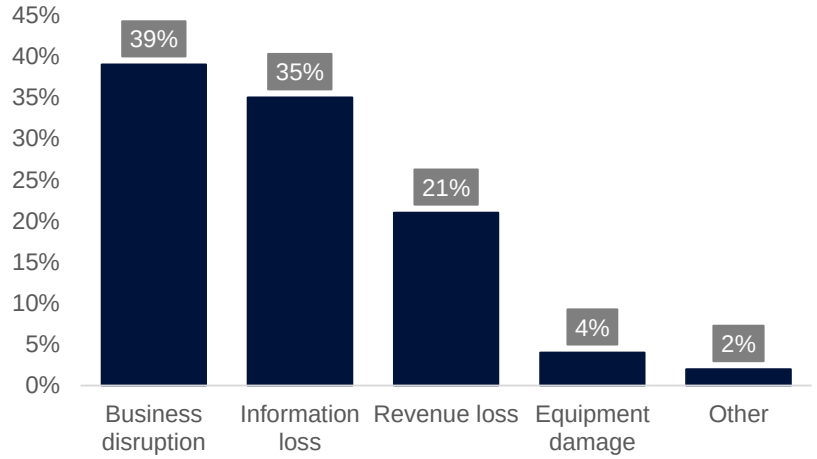

Figure 5.3: Percentages of costs per external consequence (Ponemon Institute, 2015)

The disruption of a business results into the highest costs, followed by the loss of information. The loss of revenue as well as damaged equipment have found to be less significant. This is in line with Suh and Han (2003) who indicated that the disruption of business processes resulted into a higher costs (or loss of income) than the replacement of damaged assets. The trend that more services will be moved towards the web strengthens the impact of a DoS attack (Information Security Forum, 2015). Recent developments in for instance the governmental- or electronical medical records, as well as the computerized control of traffic lights have brought a lot of advantages. But as the reliance on those services grows, the impact when these services suddenly become unavailable grow as well (Pfleeger et al., 2015).

The loss of information due to a cyber risk results into the second largest costs. This could be due to the loss of the intellectual property (IP) and therefore a reduced business advantage (Choo, 2011). The difference between the impact of such risks and for instance the disruption of a business process is closely related to the business model of the organization. An organization that manufactures products is probably more anxious that their IP gets stolen than a for instance a web shop, where the web shop is probably more focused to keep their web shop online and available (Pfleeger et al., 2015). This short example demonstrates into the fact that there is no 'one size fits all' security approach (Verizon Enterprise, 2015). Although there is some overlap between the different industries and subsectors, the relative impact of a cyber risk is based on the organization at stake.

5.4 THREAT AGENTS

PWC (2015) identified four different adversaries that initiate cyber risks. These adversaries are: Nation states, organized crime, hacktivists, and insiders. These four groups are comparable to the research of ENISA (2013) who identified nine different attackers. This selection is expanded with the notion of black-, grey-, and white hat hackers. The color notions determine the intent of the hacker (Moore, 2010). The overview of those threat agents is divided between organized cyber-crime agents (Table 5.1) and other threat agents (Table 5.2). Within both of those tables are the motives and the methods of each agent provided.

Table 5.1: Organized cyber-crime threat agents

Threat Agent	Motive	Method
Nation States	Gather information, spy on other countries to gain economic, political, and/or military advantage.	Gather state secrets, military secrets, intelligence data, or threaten the available technological infrastructure.
Corporations with malicious intent	Gain competitive advantage.	Gather competitor's business intelligence, breach intellectual property rights or gathers confidential information.
Cyber Terrorists	Influence decisions/actions of states towards their politically or relationally motivated objectives.	They may use technology both as a mean and target of their attack. They select targets that generate a lot of impact to generate the needed pressure. (for instance traffic controls, or military infrastructures)
Cyber Criminals or black hat hackers	Obtain profit from illegal activities in the cyberspace.	They act in the cyberspace and are mainly focused on financial fraud. They make use of (provided) malware, botnets, and other malicious tools and can work in globally connected groups.
Cyber Fighters	Protect their national, political, or religious values.	They initiate cyber risks in a coordinated manner. The content of the attacks can vary a lot.
Online Social Hackers	Obtaining false trust relationships to gather the needed knowledge to enter a system or building.	Use their knowledge of social engineering to generate false trust relationships. This knowledge can be combined with limited technology knowledge.

OWASP (2015a) provides a classification of threat agents based on their skills, motive, opportunity, and size. Based on this classification, can the agents from Table 5.1 be seen as highly motivated, and moderate to highly skilled groups or individuals. The common denominator is the fact that all of these agents are organized to achieve a certain malicious goal together. The specific motive, as well as the size, of these different threat agents however varies.

The remaining threat agents are hacktivists, grey- and white hat hackers, script kiddies and internal employees, these agents are described in Table 5.2. These agents vary from the agents in Table 5.1 on their intent and level of organization. This however does not indicate that these agents should, or could be underestimated. Brockett, Golden, and Wolman (2012) indicated that a large amount of the cyber-crimes come from within (internal employees) rather than outside of the organization. A side note on that

statement by Lund et al. (2010) is the fact that these internal facts could be caused by accidents instead of intended malicious intent.

Table 5.2: Other cyber threat agents

Threat Agent	Motive	Method
Hacktivists	Get media attention to spread their ideology.	Select targets that will generate high visibility after a successful cyber risk.
Grey hat hackers	Research and improve security.	The grey hatter will actively look for weaknesses in system designs and break into the system without permission. They will however not exploit the data or tell others how to do it.
White hat hackers	Test a systems security on request	A white hat hacker performs penetration tests, and other hacking practices, towards an organization or system on requests of the organization. They assess the level of security and can provide the organization with the needed advice to improve their security.
Script Kiddies	Thrill seeking, although they could be influenced by cyber criminals or hacktivists.	Their attacks are often based on DDoS and code injection attacks.
Employees/ Internal	Malicious intent is mainly caused by dissatisfaction, frustration, dissent, or corruption.	May vary significantly from lax handling, errors, towards malicious intent. They need a limited technical knowledge due to their graded access rights towards various assets in the organization.

Although the above displayed tables provide a broad overview of different threat agent it is often difficult to match an agent within only one of those categories (Pfleeger et al., 2015). It is therefore important to stay aware of the different motives, abilities, and resources that a threat agent could have.

5.5 Cyber resilience abilities

An organization is cyber resilience when it is able to defend and guard itself from the cyber threats and threat agents mentioned in the sections above. The process to become resilient includes three iterative stages (Linkov et al., 2013). These stages include a plan and prepare stage which lays the foundation to keep the assets and systems available after a cyber risk occurred. The second stage is the absorb stage, this stage occurs when a disruptive event, a malfunction or an attack, is initiated. The focus of this stage is to keep the most critical services and assets available during the incident. The third stage is aimed to recover and adopt from the impact of an occurred cyber risk. Adoption is aimed at altering/reconfiguring the systems or train/instruct the employees with the gained knowledge to prevent such risks from occurring in the future. A phase that is not included in Linkov et al. (2013) is a testing phase. A testing phase indicates that the planned security strategy is actually working as proposed. This step is included

The above mentioned stages from Linkov, Eisenberg, Plourde, et al. (2013) include different instructions on a physical, information, cognitive, and social level. These stages are in more detail described in below and followed by a section on knowledge sharing in the field of cyber risks and attacks.

5.5.1 PLAN AND PREPARE

The first stage of Linkov et al. (2013) includes the preparation phase before an actual cyber risk occurs. The physical preparation should be focused on the implementation of controls on the most critical assets and services as well as providing redundancy in the critical infrastructures and data assets (Linkov et al., 2013; NIST, 2014). Another important preparation towards cyber risks is the training and preparation of the employees (Verizon Enterprise, 2015). This control is mainly effective with social related cyber risks such as phishing mails.

Muckin and Fitch (2015) proposed eight steps, divided over two goals, to become more resilient. At first an organization should discover their specific situation. This includes the identification of their assets, the attacker's surface and attack vectors, a decomposition of their systems, and possible threat actors. Based on the gathered information they should implement a suiting risk analysis approach, perform a risk triage, and deploy controls.

Table 5.3: IDDIL/ATC methodology to be more resilient (Muckin & Fitch, 2015)

Task	Goal
Identify assets	Discovery
Define the attack surface	
Decompose the system	
Identify attack vectors	
List threat actors	
Analysis	Implement
Triage	
Controls	

A more elaborated approach to assess your current state of cyber security next to your desired state could be performed with the Deloitte Cyber Resilience Framework. This framework provides organizations an overview of their current IT situation, possible vulnerabilities, and related cyber threats. Due to the fact that the IT capabilities of the specific organization are included, the analysis will be tailored towards their needs. The framework is based on the ISO 27001 standard (ISO /IEC 27001, 2013), the NIST cyber security framework (NIST, 2014) and the SANS CIS security controls (SANS Institute, 2015). This framework combines these standards and controls and guides the user into the identification of their current situation and the needed controls to become more resilient. Due to the scope of this research only a part of the framework is described below.

The framework identified the different threat actors that potentially cause harm towards an organization. They identified ten different kind of threat agents, which can be divided over five different motivations to initiate a cyber risk. The threat agents are comparable to the ones identified in Chapter 5.4. The motives, provided in Table 5.4, provide insights and allow a certain categorization of possible cyber risks.

Table 5.4: Categories and elements in the Deloitte Cyber Resilience Framework

Category	Motives	Targeted assets	Possible impact
Elements	Making a statement	Financial Data	Financial loss
	Gain competitive advantage	Intellectual Property	Reputation harm
	Espionage	Sensitive Operational Information	Lawsuit
	Disruption	Services	Regulatory sanctions
	Financial gain	Brand image	Loss of trust
			Continuity of service

Assets that can be targeted by a threat agent as well as the possible impact are discussed next the threat agents and their motivation are discussed. Table 5.4 provides an overview of the assets and the possible impact a cyber risk can cause. It is possible that a risk can target more than one asset and/or result into different kinds of impact.

Another interesting aspect of the framework is how the cyber risks are categorized. Risks are mapped and divided between: known and understood, known but not understood, and unknown and no understanding as well as between risks that need to be prevented and risks that need a proper response plan. This categorization allows an organization to identify risks that need to be prevented, risk that are and are not understood, and to provide an indication of how resilient their organization is towards those risks.

A final note to this section is the mitigation fallacy, this indicates that it is often assumed that applied risk controls or mitigations will be performed perfectly. This fallacy can be found in several risk management standards, they assume that once a mitigation is put into place it will be performed just as planned (Fenton & Neil, 2013). Since this is not the case, it is needed to take a certain chance of failure into account when a control or mitigation tactic is planned. The next section describes an approach to determine the success of the existing controls: test and assess.

5.5.2 TEST AND ASSESS

As mentioned in the beginning of this chapter is the testing phase not part of the stages of Linkov et al. (2013). It is however, partly due to the perfect control/mitigation fallacy explained in the previous section, needed to assess the actual state of your security. There are several possibilities to test and assess the cyber security of an organization. There are for instance hacking services provided by Deloitte. These services are aimed at testing the cyber security of organizations. These hacking services include hacking tests, red hat teaming exercises, and phishing-as-a-service and are further described below.

HACKING- AND PENETRATION TESTS

A penetration test, tests the digital security of a certain IT system. These test are performed by, the in Chapter 5.4 mentioned, white hat hackers. These hackers will try to gain access an organization's IT system on request. This allows the organization to test the security of these systems. These hacking attempts are tailored towards the specific situation, but follow a general approach. This approach as performed within Deloitte is described below.

Step 1: Determine your role, and goal

Before every hack is the specific role of the hacker determined. These roles include external and internal threats towards the organization. After this role is defined, is the goal of the hacker determined. This goal usually includes a certain asset of the organization and is usually determined by the organization that requested the penetration test.

Step 2: Identify the path towards your goal

This step includes the identification of possible paths from the current situation of the hacker towards the, in step 1, determined goal. These paths usually consist of multiple steps, or hurdlers that need to be overcome. The identification of these paths is most of the time based on the experience of the white had hackers.

The identification of these paths always starts by identifying the specific situation of the targeted organization: the IT systems, security practices, and known other hurdles that you need to by-pass. This knowledge, together with the experience of previous hacks of the attacker, should result into several possible paths that an attacker could take to reach his goal.

Step 3: Select the best paths and start the hack

Based on the created paths are the best suiting paths chosen that will be used during the hack. It is however not the case that an attacker is limited to this predefined path. A hacker will learn more about the different systems and security measures during the attack, and he/she will use this knowledge when he/she pursues the attack. Due to this case, it is hard to plan or predict the exact path of an attacker.

RED HATTING TEAM

The red hat teaming exercises are, in contrast with penetration, or normal hacking tests, not limited towards digital access. Their exercises could include gaining physical access to the office or data center of an organization. A Red teaming attack simulation therefore provides a broader cyber security overview than a regular hacking exercise.

Within the red teaming they make use of general attack graphs of possible attacks. These graphs are used as a starting point for the real attack. The purpose of those diagrams is therefore not to provide details of the proposed attack (Cheung, Lindqvist, & Fong, 2003). These diagrams are comparable to the 'hacking' paths described in the section above, but they entail a broader scope.

PHISHING-AS-A-SERVICE

As mentioned in Chapter 2.1.3 Deloitte performs phishing-as-a-service towards their clients. This service simulates a phishing attack towards a specific organization to test the vulnerability of the different departments towards phishing. This service makes use of spear-phishing mails, which are targeted towards an individual, department, or organization, to gather information which could be used to enter a for instance the organization's systems. The use of such spear phishing is usually performed in one of the three ways described below:

1. The recipient is asked for his username and/or password (this can be direct, or indirect by directing them to a website). A problem with this kind of attack is the fact that external websites are out of the scope of the IT department and therefore difficult to control and block if needed.

2. Malicious software is attached in the mail; this can be hidden within another attachment. These kind of malicious attachments are more difficult to identify as a user, but can be identified and blocked by the IT department.
3. The third way is less known, but also more difficult to detect. The threat agent that sends this kind of phishing message pretends to be for instance a recruiter to obtain résumés of people within the IT department. These documents will provide a lot of personal information on the employees as well as technical information which could indicate the type of systems and technologies that are deployed within the organization.

The effectiveness of a phishing mail relies on both the quality of the mail, and the awareness of the receivers. It is therefore difficult to estimate an average success rate of such phishing mails. The estimation provided by Verizon that 23% of the recipients of a phishing mail will open it, and 11% will even click on the attachments (Verizon Enterprise, 2015), seems in line with the findings of Deloitte's phishing-as-a-service. These numbers indicate that when a phishing campaign with only 10 spear phishing e-mails is initiated, the chance that none of these employees open the mails is only 7.3%. These kind of phishing mails form the basis of more than two-thirds of cyber espionage incidents (Verizon Enterprise, 2015). A disadvantage of such numbers is that they are highly dependent on the contextual situation of the targeted organization and individuals as well as the quality of the phishing mail.

Besides the phishing attempts to gather information to gain access to a system, there are direct financially motivated phishing attempts. There are a lot of different possibilities and examples to attempt these kind of actions. They range from mass phishing mails that ask for credit card credentials or to transfer money directly to a certain account, towards targeted attempts to deceive an employee that you are the CEO and that he/she should transfer money of the organization towards an account. Threat agents can be creative and persuasive with their reasons to convince the employee that the action is legit.

5.5.3 INCIDENT RESPONSE

Incident response overlaps with the absorb and recover phases of Linkov et al. (2013), this indicates a quick identification, as well as a proper response, when a certain risk occurs. An important aspect is to isolate the infected systems, and to replace these systems with back-up systems (if they are available) (Linkov et al., 2013). This will make sure that the business disruption remains as minimal as possible.

Another important aspect is preparing instructions towards the employees when such a threat occurs (Linkov et al., 2013). This will speed up the response process and will therefore minimize the consequences of the risk as much as possible. These instructions will be captured in an incident response plan. Such a plan should define when something is considered an incident, the responsible employees that will take charge of the situation, and at last a plan of action (Pfleeger et al., 2015).

5.5.4 RECOVER AND ADAPT

The last stage after a security incident is the recover and adapt phase (Linkov et al., 2013). These phases should include the restorations of all the assets, business processes, and software systems to their normal use, as well as providing some sort of incident review to assess the current level of security (Pfleeger et al., 2015). The recovery phase includes decision making around the needed recoveries. A recovery planning should guide this process to ensure a correct and timely restoration of the affected systems and assets (NIST, 2014). The recovery plan should consist of concrete restoration activities, which should be coordinated with the needed stakeholders.

The adaption phase of Linkov et al. (2013) aligns with the incident review as described by Pfleeger et al. (2015), and the improvements and communications phase of the NIST framework (NIST, 2014). This phase includes the incorporations of lessons learned from a certain risk to benefit future incidents. These lessons can be identified by the incident review, which focuses on the taken security controls, as well as an investigation to possible control failures or gaps. Another element that is needed to consider is the effectiveness of the incident response plan. This review should identify if the plan was followed correctly, and if not what the reason was that it was not followed (Pfleeger et al., 2015).

Another approach to learn from occurred incidents is to create a repository to store those incidents. These incidents could then be used to identify the vulnerable aspects within the organization. They could also be used to assess the current state of security; this indicates that an organization walks through the steps of the incident to test if it could still occur. In order for the repository to be useful and successful it should capture all the relevant details of the risk. Within Deloitte is a shared cyber case repository which contains several cyber incidents. The purpose of the Deloitte repository is however different as described above. It is created to capture example cyber incidents which could be used to emphasize the different possibilities of cyber risks and therefore the importance of proper cyber security. The cases within the repository are, as described in Chapter 2.1.3, captured in the proposed cyber risk taxonomy to evaluate the preliminary versions of the taxonomy with real cyber incidents. An overview of the described components within the repository is provided in Appendix H.

5.6 Conclusion

The entire environment in which communication between, or via, computers exist should be defined as cyberspace. This environment is growing, but alongside this growth in opportunities are the accompanying risks growing as well. These cyber risks grow both in numbers and in sophistication. It is possible to divide cyber risks within defined categories. Clough (2010) divided these cyber threats between unauthorized computer access, use of malicious software, and disruption of business processes.

Disadvantages of the Clough's categorization is that the categories are at a very high level and not mutually exclusive. This is mainly the case for the use of malicious software, which is often used to achieve unauthorized access to- or the disruption of a computer system. This research therefore identified other cyber risk categorizations, which resulted in several categories with different levels of detail and focus. These categories include the cyber kill chain (Lockheed Martin Corporation, 2015), which divides the threats based on their stage within an attack, or the STRIDE-LM and IRAM2 categories, which have more overlap with Clough (2010), but provide more detail, and IRAM2 even provides pre-defined controls per risk category to prevent or mitigate these risks.

The impact towards an organization of cyber risks, depends highly on the organization's business. For instance, a production organization with valuable digital intellectual property is more harmed if this information is stolen by a competitor than online retailer, who will be focused on the availability of his online shop and therefore the continuity of his business processes. An overall research of the Ponemon Institute (2015) indicated that the biggest financial impact of cyber risks is caused by disrupted business processes, followed closely by lost information. Studies conducted by Pfleeger et al. (2015) and Suh and Han (2003) confirmed this finding.

The fourth section of this chapter identified eleven different existing categories of threat agent. Although these threat agents vary in their motivation, resources, or skills, there is a lot of overlap as well. This overlap,

together with the difficulty to identify these elements, makes it difficult to categorize threat agents. The variables however remain important to identify the potential threat agents in the threat landscape.

The last section of this chapter described approaches an organization can take to become cyber resilient. These approaches follow four generic steps that include the entire lifecycle of a cyber incident. At first is a plan and prepare phase, which goal is to prepare an organization for potential risks by performing analyses and deploying needed controls. The second step, test and assess, is included to test the deployed controls. The third step, incident response, is aimed at a quick a proper response during a cyber incident to minimalize the impact. The last step is recover and adapt, during this step is the incident and the incident response evaluated to learn from it. The goal of that last step is to further improve the organization's cyber security.

6. A CYBER RISK TAXONOMY

The structure of the cyber risk scenarios will, as explained in the research approach, be provided by a risk taxonomy. The risk concepts, identified in Chapter 4.2, form the basis of the current taxonomy. This basis is further elaborated with several models and approaches to provide a taxonomy that describes the entire scenario of a cyber security risk. The provided concepts are further elaborated with several characteristics to provide more details about these concepts. The eight different concepts and 51 characteristics are described in Section 6.1 below.

6.1 CONCEPTS WITHIN THE CYBER RISK TAXONOMY

The created cyber risk taxonomy is based on a scenario based risk approach. Such an approach indicates that a risk is not a single event, but rather a sequence of events that together causes a negative consequence (Fenton & Neil, 2013). The scenarios are further elaborated with contextual information about the victim and threat agent to identify all the relevant concepts within the scenario. The approach to gather these elements is comparable to the research of De Kock (2014), who intended to structure acts of terror to analyze terrorist behavior. The taxonomy is, besides the story elements of De Kock (2014), based on the risk scenario concepts that were identified in Chapter 4.2, and the STIX structured cyber language (Barnum, 2014). The combination of these three approaches has resulted in a comprehensive and complete cyber scenario taxonomy. The story elements of De Kock (2014) are tailored towards cyber incidents, and are more focused towards the causal events within the risk scenario. The risk concepts that were defined in Chapter 4.2 (Figure 4.1) provide the basic structure of the taxonomy, but are elaborated with several variables to provide a more detailed structure. The STIX language provided important and detailed cyber related insights, those insights are elaborated with causal and contextual risk scenario information.

Table 6.1: The number of variables in the cyber taxonomy

Concept	De Kock reference	Risk concepts (Chapter 4.2)	STIX reference	No
General information	Arena & Time (frame) & Context		Indicators	8
Organization (victim)	Protagonist		Indicators	5
Threat agent	Antagonist & Motivation	Threat agent	Cyber Threat Actors	5
Asset	Primary objective	Asset	Cyber Observables	9
Threat event	Means & Modus operandi & Red herring	Threat event, Risk event	Cyber Attack Campaigns & Adversary Tactics, Techniques, and Procedures (TTP)	8

Business impact		Technical- and business impact	Incidents	5
Vulnerabilities		Vulnerability	Exploit Targets	6
Control	Resistance	Controls and mitigations	Courses of Action	5
Total				**51**

The risk and cyber literature that is described in described in Chapter 3, 4 and 5, together with the Deloitte hacking practices (Chapter 5.5.2) is used to construct the variables that describe the concepts in more detail. The different concepts, and an overview of the amount of variables per concept, are provided in Table 6.1.

It is important to note that each concept should be present within the description of a cyber risk scenario. Each concept therefore contains a numeric key to indicate the scenario it adheres to. It is however possible, and most likely, to have multiple threat events within the scenario. The vulnerabilities and controls are related to the threat events, it is therefore possible to include multiple vulnerabilities and controls within scenario. The remainder of this section will elaborate on the variables of each concept in Table 6.1. For each variable is a description and a type provided. The type indicates if the variable is an integer, textual description, category, or a scale. Appendix B provides an overview of all the categories and scales that are used in the taxonomy.

Table 6.2: General scenario information

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
Description	A short description of the story within this scenario	Text
Goal	The goal of the initiator of this scenario	Text
Year	The year this scenario took place	Integer
Quarter	The quarter within the year this scenario took place	Integer
Timeline	An indication of the duration it took to control this incident	Category
Scenario type	An indication if the scenario is designed for risk analysis purposes or a real occurred incident	Category
Scenario plausibility	An indication of the plausibility that such an incident would occur	Integer

Table 6.2 provides an overview of the different characteristics of the first concept. These characteristics should provide a quick overview of the story of the risk scenario as well as when it took place. The year and quarter indicate when the incident occurred, and timeline indicates the duration of the occurred incident. The scenario type characteristic indicates if the modeled scenario is an occurred incident or created for pro-active risk analysis purposes. Chapter 7.3 describes how the taxonomy could be used. This includes both the identification of occurred incidents and the identification of possible risk scenarios for risk analysis purposes. The last variable indicates the plausibility that this scenario will occur, which is determined by the underlying factors. The estimation of this value is further elaborated in the next chapter about the cyber risk scenario model.

Table 6.3: Organization information

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
Industry	The industry in which the organization operates	Text
Type	A more specific description of the organization's business	Text
Size	An indication of the size of the organization, the size is indicated by the number of employees	Category
Location	The country/ region where the organization operates	Text

The organizational information provides more contextual information about the organization that was harmed by the incident. This contextual information can be used to indicate if a certain threat is relevant towards another organization. This description is focused about the industry, type, size, and location of the organization.

Table 6.4: Threat agent

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
Type	The type of threat agent that initiated the cyber risk	Category
Motivation	The goal of the threat agent	Category
Skills	An indication of the skills of the threat agent	Scale
Resources	An indication of the resourcefulness of the attacker	Scale

The threat agent within a cyber risk scenario is the initiator of the threat events and therefore the cyber risk scenario. The categorization is based on the more elaborate categories described in Table 5.1 and Table 5.2 in Chapter 5.4. The categorization is decreased due to a large overlap between the characteristics of the several threat agents. The remaining agents have proven to be broad enough to capture all the threat agents within the data of this research. The categories are specified by adding the motivation of the agent. The categorization and motivation are elaborated with an indication of his skills and resources. The indication of the agent's skills and resources are based on the risk rating methodology of OWASP (2015a), and are captured, together with the other categories and scales in Appendix B.

Table 6.5: Asset

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
Description	A general description of the asset that has been targeted	Text
Category	The type of asset	Category
Accessibility	An indication if the asset could be accessed by everyone, or a select group of users	Category
Source	The storage device, or system, on which the cyber asset was stored	Text
Other breached sources	Other assets or systems that were breached in order to get to the desired asset	Text

Encryption	An indication to tell if the cyber asset was encrypted when it was stolen	Category
Value internal	An estimation of how valuable the asset is towards the organization	Category
Value external	An estimation of how valuable the asset is towards a potential external party	Category

Each scenario that is captured within the taxonomy is focused towards a certain asset of the organization. Each asset is categorized, these categories are based on the Deloitte cyber resilience framework (Chapter 5.5.1), Choo (2011), and the Information Security Forum (2015). This predefined categorization is included to provide more structure than the free-form description of the asset. The remainder of this concept is focused towards the accessibility and the source of the affected asset. This is included to provide an overview of how the asset could be accessed, and what systems were breached to reach the asset. Besides the encryption characteristic, which indicates if the asset (in case it is data/information related) is encrypted, is an indication of the value of the asset provided for both the organization itself and a potential external hacker.

Table 6.6: Threat event

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
ThreatID	A key to indicate the specific threat event	Integer
Description	A general description of the threat event	Text
Stage	Indicates the stage within the cyber attack	Category
Type	A category that indicates the specific threat event	Category
Technical impact	Indicator of the technical impact that the threat event causes to the organizations systems	Category
Sophistication	A technical sophistication indication	Scale
Modus	The way in which the threat event was performed	Category

Threat events are a central concept within a cyber risk scenario. These events are initiated by the threat agent (described in Table 6.4). It is possible to enter multiple threat events per scenario in the taxonomy. This is possible due to the fact that each threat event has both a ScenarioID as a ThreatID, to identify both the specific threat event, as the overall risk scenario. To further specify the specific threat event, it is possible to include the stage within the cyber risk. These stages are based on the cyber kill chain of the Lockheed Martin Corporation (2015) which is described in Chapter 5.2.4. A difference between Lockheed Martin's approach and this approach is that this approach does not require an attacker to follow each step in a linear manner. As described in Chapter 5.5.2, a cyber risk is very iterative and dynamic, and an attacker could for instance need more information in a later stage of its attack and therefore perform a reconnaissance stage after an exploitation stage.

There is a threat type assigned to each individual threat event to complement the stage. These stages are based on the IRAM2 framework (Information Security Forum, 2014). Besides providing more detail of about the specific threat event, it is also possible to make an estimation about the sophistication of the threat event, as well as creating a link with pre-defined controls. Both the controls and sophistication estimations

are provided within the IRAM2 framework (see Appendix A for the different threat types and sophistication levels).

The final characteristics of a threat event indicate the technical impact the event causes, and the modus of the event. The technical impact indicates the result of the event towards the system (OWASP, 2015a). This could be a loss of confidentiality when information could be accessed, or a loss of integrity when the correctness of certain information could not be ensured. The third type of technical impact indicates that it is possible to lose the availability of a certain system, server, or service. At last is the possibility that a threat event causes a loss of certain security measures. These four different kinds of impact could be achieved in four different ways: social engineering, malware, hacking, or a physical attempt.

Table 6.7: Business impact

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
Description	A general description of the business impact that is caused by the scenario	Text
Financial	A relative indicator of the financial damage	Scale
Non-compliance	A relative indicator of the organization's compliance, or violation, of the regulatory standards	Scale
Reputational	A relative indicator of the amount of reputation damage that could result due to this scenario	Scale

The business impact is described with both a qualitative description and quantitative estimations. The quantitative estimation is based on the risk rating methodology of OWASP (2015a) and consist of three rating scales: financial damage, reputational damage, and non-compliance. These measures provide an overview of the relative severity of the total risk scenario. More details about the impact could be added in the free-form textual description of the business impact.

Table 6.8: Vulnerability

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
ThreatID	A key to indicate the related threat event	Integer
Description	A general description of the vulnerability that has been exploited	Text
Type	A rough division between social and technical vulnerabilities is made	Category
Ease of exploit	A relative indication of how easy an attacker could exploit this vulnerability	Scale
Awareness	A relative indication of the internal awareness of this vulnerability	Scale

Vulnerabilities could be identified based on the threat events within the risk scenario. The vulnerabilities are exploited in order for a certain threat event to be successful. It is therefore possible to define multiple vulnerabilities within one cyber risk scenario. On the other hand, it is not obligated that each threat event

is combined with a vulnerability. The concept consists, as presented in Table 6.8, of a description, type, and two scales. The type indicates if it is a social, or technical vulnerability, where the scales indicate the awareness of the vulnerability and the ease of exploit.

Table 6.9: Control

Variable	Variable description	Type
ScenarioID	A key to indicate the specific scenario	Integer
ThreatID	A key to indicate the specific threat event that is countered by this control	Integer
Description	A description of the control that was applied	Text
Type	An indication of what kind of control it is	Category
Relative costs	An indication of the costs of such a control	€

The last concept within the taxonomy is the control, which is further described with a description, type, relative costs, and a specific threat that it controls. With the control type is a distinction made between detective, preventive, and reactive controls. Detective controls include IT monitoring, and allows an organization to identify possible threats as soon as possible. Preventive controls can be seen as the standard security capabilities (e.g. the use of two factor authorization, encryption, and physical security of the organization). The reactive controls are the actions that an organization will perform when a threat has occurred, and they aim to mitigate the impact as much as possible.

6.2 Creation of a cyber risk scenario

A risk scenario captures the most relevant elements within the cyber taxonomy. The goal of such a scenario is to identify and describe the different events that together cause a negative impact to the organization. Such a risk assessment is in contrast with risk assessment that focus on the risks of an organization with atomic threat events. The overview of the different threat events provides the ability to identify the different possibility to control a cyber risk by identifying the different vulnerabilities or weaknesses that an attacker will need to exploit in order to reach his goal. The creation of these scenarios is based on the three general risk analysis steps: identify, describe, and estimate (IRM, 2002).

6.2.1 Identify the taxonomy concepts

As described in Chapter 3.1, there are three different approaches to identify risks within a situation. These approaches focus either on the threat, the organization's assets, or the vulnerabilities. The same chapter indicates that Pfleeger et al. (2015) state that a reliable risk identification process should focus on all of these elements. The proposed scenario based risk analysis complies focuses on all of these elements and therefore complies to the risk identification requirement of Pfleeger et al. (2015). Given the amount of time it takes to identify all the elements within the taxonomy, should only the more advanced threats be included. These advanced threats (or APTs as described in Chapter 5.2) include multiple threats and they do not have a predefined fix or control, and are specifically targeted towards a specific organization (or multiple organizations).

The first taxonomy concepts that should be identified are the ones that describe the organization and the contextual situation. It is important to determine the asset that is at risk for the specific scenario. Each scenario should be focused at one specific asset, but each asset could be harmed by multiple scenarios. When the asset is identified it is possible to identify to what extent potential threat agents that are

motivated to initiate an attack. By doing so, it is possible to focus on the asset's value towards the organization as well as the potential threat agent.

Once the asset has been identified it is important to focus on the IT landscape around the asset. The identification of the systems that are connected with the asset provides an overview of the different ways a threat agent could reach the asset. Based on the needs of the risk analysis the amount of detail of the IT landscape can vary from an overview of the connected systems towards a detailed overview of the possible network traffic and network security measures. Information about the IT landscape could be gathered from enterprise architecture documents and/or IT owners/responsible persons.

After the asset and the IT landscape are identified it is possible to identify possible paths an attacker could take to reach its goal, comparable to the hacker's approach (Chapter 5.5.2). There are several pre-defined lists, see Chapter 5.2.4, of cyber threat actions available to guide the identification of these paths. Besides these lists of threat actions, it is also possible to use earlier created or identified threat scenarios for the identification. These scenarios are accessible in a repository that allows a user to query for specific risk scenarios that are comparable to his situation. This specific use of the cyber risk scenario is further elaborated in Chapter 7.3.

6.2.2 DESCRIBE THE RISK SCENARIOS

After the different concepts and characteristics within the taxonomy have been identified, it is important to properly describe the causal structure of the different threat events within the scenario. This causal structure provides an overview which is needed to identify the most crucial risks as well as the control possibilities. The needed overview could be provided by incorporating a causal model, as described in Chapter 4.3. A causal model provides an overview of the relations between the different events and concepts of the scenario. The identified causal chain of events, together with vulnerabilities and controls, provide an overview of the different steps an attacker should take in order to get to his goal (the organization's asset). This chain allows the assessment of the organization's security, by identifying possible vulnerabilities. The different characteristics in the taxonomy allow for both qualitative (descriptions) as quantitative (scales) measures of the threat events and vulnerabilities. The quantitative measures can be used to estimate an overall probability value that indicates the chance that the risk scenario actually occurs.

6.2.3 ESTIMATE AND MODEL THE SCENARIO

Causal models can be used to capture quantitative measures to determine overall probability and impact estimations. These measures could be used to indicate the 'value' of each risk scenario (see Chapter 3.3). These risk values allow an organization to prioritize their cyber risk scenarios. Chapter 7 elaborates on the application of a causal model to the cyber risk taxonomy. The information that is captured within the taxonomy is used in the construction of these causal model.

A risk assessment is, as indicated in Chapter 3.3, often based on an impact and a probability value. The business impact of the cyber risk scenario can be assessed with the scales that are provided in the taxonomy. These scales include three different characteristics: financial impact (both direct and indirect), compliance violations, and reputational damage. These three different characteristics, which are based on the OWASP risk rating methodology, provide an overall business impact estimation. The scenario's probability estimation is based on the threat agent's capabilities (method), asset attractiveness (motivation), and the threat event's sophistication (opportunity). These elements provide an overview of the three components that influence the possibility of a criminal act (Byres & Lowe, 2004; Choo, 2011; Cohen & Felson, 1979; Pfleeger et al., 2015). Due to the fact that a cyber risk can be seen as a criminal act, are these factors used

to estimate the scenario's probability. The taxonomy captures several characteristics to assess these three components. These values can be assessed within a causal model that indicates the probabilistic dependency between these three different components. The application of such a model is explained in the following chapter.

6.2.4 DEPLOY CONTROLS WITHIN THE SCENARIO

Once the scenarios have been constructed it is possible to identify the vulnerabilities within the organization's IT landscape. By controlling these vulnerabilities, the probability and impact of an incident will be decreased. An advantage of the identified causal chains is the possibility to identify the best moment to control certain risks within the causal chain of the incident. The specific control tactics are not within the scope of this research. There are however several cyber risk control frameworks that provide good control indications for specific threat events (e.g. STRIDE-LM and IRAM2, see Appendix A), as well as general frameworks with cyber risk controls (e.g. CIS critical security controls (SANS Institute, 2015)).

An organization should re-assess the scenario once a control has been deployed. This results into a new overview of the probability and impact of the scenario. This assessment is a good indication to justify the investment of certain control measures. It should however be noted that implemented control measures are never flawless and could fail (see Chapter 5.5.1).

6.2.5 STORE AND REUSE THE SCENARIOS

The taxonomy could, besides the risk assessment and analyses possibilities of the taxonomy, be used to store the identified cyber risk scenarios in a structured manner. The proposed elements, and their variables represent the data structured that could be incorporated in a repository. Such a repository should allow an analysist to query or filter for scenarios in the repository that match specific needs. These queries and filters can be based on the contextual factors, to identify cyber risks in a similar situation, or they could be based on the technical aspects of the risks to identify possible cyber risks or the possible impact of such a risk.

The structure of the taxonomy allows the above mentioned possibilities to search for specific scenarios in a repository. These scenarios, or parts of the scenarios, could be used to create a new scenario. It is important for such a repository to contain a significant amount of scenarios in order to be usable. Cyber risk related knowledge sharing, as described in Chapter 3.1.4, is one way to increase the amount of scenarios in a repository.

In this research is the structure of the taxonomy captured within an Excel sheet as a proof of concept (this is further explained in Chapter 8.2). This proof of concepts allowed us to validate the structure with the cyber incidents from the Deloitte cyber risk repository. The Excel sheet however did not provide the above mentioned capabilities to filter or query through the different scenarios.

6.3 CONCLUSION

The above described taxonomy captures all the relevant elements of a cyber risk scenario. By capturing all these elements in a structured manner we provide an overview of the entire story of the specific cyber risk (Barnum, 2014; Roxburgh, 2009). The elements are gathered from various sources ranging from general risk models, terrorist behavior models, and cyber specific models. The combination of these different models resulted in a taxonomy that is able to capture cyber risk scenarios.

The proposed taxonomy contains eight concepts, which are described by 51 variables, to capture the entire story of the risk. The different concepts, and their variables could be captured within a data model to capture

multiple scenarios within this structure. This structure provides, as indicated in the problem statement of this research, the ability for knowledge reuse and the creation of an organizational memory (Nonaka, 1994). A second advantage of the taxonomy is that it is able to capture multiple threat events within one threat scenario, which is needed to capture the dynamic structure of cyber risks. These multiple threat events are combined with the different contextual concepts in the taxonomy to provide a complete story of the risk.

A minor limitations of the current threat events within the taxonomy is that it does not explicitly represent the causal structure, or probabilistic dependency, between the different threat events in a scenario. This is because the focus of the taxonomy is towards capturing the entire story of the risk. An overview of the structure between these threat events is useful to identify, which threat events should be controlled or mitigated in order to control the overall risk scenario in the best way possible (Fenton & Neil, 2013). To include this causal structure of the different threat events within this research, it is applied to several causal models in the next chapter. These models provide an overview of the structure, as well as an indication of the probabilistic dependency between them. Another possible limitation is the high level of detail of the taxonomy. This detail is however needed to capture the entire story of the cyber risk scenario (Barnum, 2014; De Kock, 2014).

7. A CYBER RISK SCENARIO MODEL

The causal relationships and dependencies between the identified threat events within the cyber risk taxonomy are, as indicated in the conclusion of Chapter 6, not explicitly captured in the current taxonomy. As indicated in Chapter 4.3, a causal model can capture the different elements as well as the relations between these elements. It is therefore an option to combine a causal modeling technique with the cyber risk taxonomy to explicitly capture the causal structure of the cyber risk scenarios.

This chapter describes the possibilities to incorporate the cyber risk structure of the identified taxonomy within a causal model. The first section of this chapter provides a short recap of the six causal models that are described in the literature review (Chapter 4.3). Out of those six models three models are selected to capture the structure of the defined taxonomy. The remainder of this chapter (Section 7.3) will describe the different ways in which these scenario models could be used.

7.1 SELECTING CAUSAL MODELS

Chapter 4.3 described six different modeling techniques to capture causal networks. As indicated above there are three models selected to demonstrate the possibility to create a scenario model out of the proposed taxonomy. The chosen techniques include Bayesian networks, the CORAS model, and ANRAM (Argumentative-Narrative Risk Assessment Model). The choice of these techniques, over the Bow tie diagram, Influence diagrams, and Petri nets is elaborated below.

7.1.1 NEEDS OF A CYBER RISK SCENARIO MODEL

The selection procedure between the different casual models is guided by four high level requirements. These requirements describe the needs of such a model in practice, and are based on the literature study and validation interviews. The needs can be summarized as follows: the causal model should capture the entire story of the occurred cyber risk in an understandable, adaptable, and user friendly manner. Existing causal models that could provide this needed overview can be divided between qualitative, semi quantitative, or quantitative models. The advantages of both the qualitative and quantitative models are summarized in Chapter 3.3.3 (Table 3.4). This research includes a qualitative model, a semi quantitative model, and quantitative model to express the specified needs that are provided in Table 7.1.

Table 7.1: Needs of a cyber risk scenario model

No	Requirement	Description
1	Dynamic structure of the scenarios	Each cyber risk consists of several threat events. The amount and order of these events can be different for each cyber risk.
2	User friendly scenario creation	A user should be able to quickly create or adjust cyber scenarios to keep up with the rapidly changing cyber threat landscape.

3	Contain complete risk scenario	It is needed to identify all the relevant concepts within a cyber risk scenario in order to provide the complete, and correct, story.
4	Understandable scenario overview	The scenario should provide a clear overview of causal structure of threat events. This overview should allow discussions about vulnerabilities and their consequences.

7.1.2 INCLUDED MODELS

As described above Bayesian networks, the CORAS model, and ANRAM are selected to capture the taxonomy's structure to model the cyber risk scenarios. These models range between quantitative-(Bayesian networks) and qualitative models (CORAS). ANRAM can, due to its understandable overview and formal logical grounding, be seen as a semi quantitative model and is therefore included in this research. The compliance of these three models with the needs of Table 7.1 is further elaborated below.

A Bayesian network is a quantitative model that combines nodes in a connected graph with quantifiable probability tables. The graph indicates the probabilistic dependency between different nodes this dependency is further defined by the probability tables. The dynamic qualitative graph, which could be further specified with the probability tables, allows a Bayesian network to comply with requirement one, three, and four. Due to the complexity, and its need for detailed and specific data in the probability tables, it is not very user friendly. This problem is however partly solved with the available software tools to create Bayesian networks (e.g. AgenaRisk (2016)).

In contrast with a Bayesian network, the CORAS model is a qualitative model. CORAS consists of both a modeling language and a risk analysis method. The aim of the CORAS models is to provide a quick and understandable overview of the possible risk scenarios. CORAS provides a model that is relatively easy to create and provides a clear overview of a specific risk scenario due to its relatable icons. Due to its user friendliness and clear and complete overview of a cyber risk scenario, CORAS complies with all four of the requirements that are defined in Table 7.1.

The third model that is included is ANRAM, which is based on the Hybrid theory (Bex, 2011). ANRAM is a qualitative risk model with a formal logical grounding. The model captures and calculates both impact and probability values for an overall scenario and for the individual events within the scenario. Besides the risk events it is possible to model evidence and claims which might affect the probability that the risk scenario will occur. These possibilities allow a user to dynamically update the risk scenarios towards the current situation. Another advantage of ANRAM is that it is designed to be applicable in the practice, which makes it a user friendly model to use. ANRAM therefore complies with all four of the defined requirements.

7.1.3 OMITTED MODELS

In contrast with the above mentioned models the Bow tie, Influence diagram, and Petri nets are omitted from this study. The Bow tie is a very generic model that is open for interpretation. Many different descriptions and interpretations of the Bow tie exist, which makes it difficult to combine this modeling technique with our taxonomy. Another disadvantage of the Bow tie model is that it is not able to capture one specific risk scenario in an understandable manner, but captures multiple possible scenarios within one diagram. The Bow tie therefore does not comply with the third and fourth requirement.

Influence diagrams are a generalization of Bayesian networks (Kjaerfulff & Madsen, 2005), and therefore share a lot of comparable characteristics. The extra characteristics of Influence diagrams provide more complexity within the model as well. This increased complexity results into a decreased user friendliness, but it does not provide extra advantages towards our desired research. Therefore, Bayesian networks are chosen over the Influence diagrams within this research.

Petri net is the third model that is omitted from this research. A Petri net is a mathematical model that consist of states and transitions. The behavior between the states, which can be defined by the transitions, is visualized by tokens in the network. This functionality allows a user to simulate the possible outcomes of a specific situation. The modeling of such a situation is time-consuming and needs a lot of detailed information about each of the possible decision points. The aim of the risk model should be to provide an understandable overview of the causal structure (requirement 4) instead of applying elaborate simulations of the possible outcomes. Another disadvantage is related to the effort and time it takes to gather the needed information and to construct the Petri net. This disadvantage is the decreased user friendliness (requirement 2). The Petri nets are therefore omitted from this research.

7.2 CONSTRUCTING A CAUSAL CYBER RISK MODEL

In this section the application of the three selected causal models to model a cyber risk scenario is described. Each causal model has its own characteristics and advantages to model a certain causal structure. These different characteristics are described and tailored in order to model a cyber risk scenario. As stated in the introduction of this chapter, one of the main reasons that causal models are included is to express the causal structure between the different threat events in a cyber risk scenario. The remainder of this section describes the application of cyber risk scenarios to express the causal structure within a Bayesian network, CORAS model, and ANRAM.

7.2.1 BAYESIAN NETWORK

A Bayesian network consist of probability nodes that are connected in an acyclic graph. The graph represent the probability distributions between the nodes in the network (Vlek, Prakken, Renooij, & Verheij, 2015), and should be acyclic to prevent circular reasoning (Fenton & Neil, 2013). Each node in the network represents a variable and for each of those variables a Node Probability Table (NPT) is constructed. These NPTs contain the different instances of a variable (e.g. TRUE and FALSE, but it could contain more instances) together with a probability value for each instance (e.g. TRUE = 0.8 and FALSE = 0.2). This section describes the construction of a graphical network as well as a NPT. After these descriptions the cyber risk taxonomy is applied to a Bayesian network to estimate the probability values within the cyber risk scenario. This section is concluded with some conclusions about this specific application of the cyber risk taxonomy.

PROBABILISTIC GRAPHICAL NETWORK

The graphical network indicates the dependencies between nodes in the Bayesian network. These relations are indicated with arrows between the nodes. The arrows are commonly directed from a certain cause to an effect, they do however represent a probabilistic dependency instead of a causal relationship (Vlek et al., 2013). The construction of this graph could be guided with idioms, which are a set of rules which can be used to create a specific part of a Bayesian network. Idioms can therefore be seen as the building blocks of which the graphical network is constructed (Neil, Fenton, & Nielson, 2000). These building blocks allows the use of idioms to incrementally create parts of models, which could later be combined into a cohesive whole (Fenton, Neil, & Lagnado, 2013).

Two idioms are used to construct a probabilistic graph that supports the cyber risk taxonomy. To capture the interplay between the causal structure of the threat events can the scenario idiom be used, as described in Vlek et al. (2013) and Vlek et al. (2015). They describe a way to use scenario schemes within a Bayesian network, which is done by creating a scenario node, and several event nodes (as displayed in Figure 7.1). The event nodes describe the different events that happened within the scenario, and the scenario node indicates if the entire scenario is true or false.

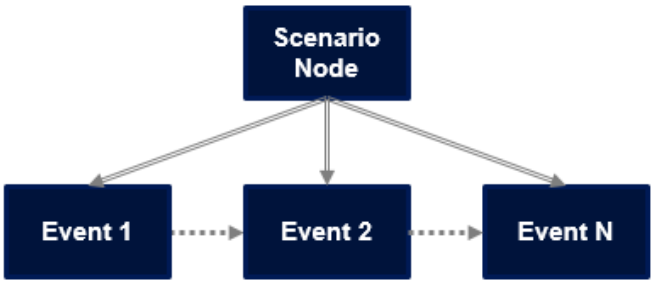

Figure 7.1: Example of a scenario node, created according to the scenario idiom

As displayed in Figure 7.1 multiple arrows are used within this idiom. The double arrows indicate a special relation between the central scenario node and the individual event nodes. These relations indicate that if the scenario node is true, each of the event nodes will be true as well (Vlek et al., 2015). This simultaneous indicates that an individual event with strong proof can positively influence the probability that the scenario as a whole is true as well.

The dashed arrows between the events indicate possible dependencies between these different events within the scenario. The dashed arrows of the possible dependencies will change to straight arrows once the dependencies within the scenario are determined. These dependencies between events are, as indicated above, not limited to causal relations. The specific relation between two events within a scenario idiom could be specified with a label: c (causal), or t (temporal) (Vlek et al., 2015). These labels indicate if a dependency is causal (A caused B to occur), or it is temporal (first A occurs, and then B occurs).

The definitional/synthesis idiom is, besides the scenario idiom, included to model a cyber risk scenario within a Bayesian network. The definitional/synthesis idiom, as described by Fenton and Neil (2013), allows the creation of a synthetic node out of multiple nodes. A synthetic node is created to organize the Bayesian network by grouping certain nodes. The grouping of nodes within synthetic nodes could be applied to the different characteristics that represent the scenario's context in the cyber risk taxonomy. An overview of a synthetic node that groups two sub nodes is provided in Figure 7.2.

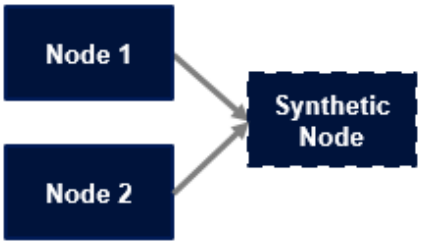

Figure 7.2: Example of a synthetic node

The Bayesian network to model cyber risk scenarios will be based on the scenario- and definitional/synthesis idioms, but adjusted where needed. The combination of these two idioms combine the necessary causal (or temporal) structure of the threat events, with the contextual information to create a complete risk story. This combination results into a complete risk scenario, that contains the needed story of the risk (Barnum, 2014).

NODE PROBABILITY TABLES (NPTS)

The probabilistic dependencies between the nodes in a Bayesian network are, as indicated above, further specified by node probability tables (NPTs). A NPT defines the probability values for each of the instances of the node (given its parents). The creation a NPT can best be illustrated with the two example Bayesian networks in Figure 7.3, which provides a node with one, and a node with two parents.

Figure 7.3: Two examples of connected graphs

The probability table of a node with one parents should define the probability value for its instances for both the instances of his parent. Table 7.2 provides an example NPT of a node with one parent and Boolean values. This table indicates the probability values when the parent node is TRUE and when it is FALSE.

Table 7.2: Example NPT with one parent node

Parent node 1:	**TRUE**	**FALSE**
Node 2 TRUE	0.8	0.6
Node 2 FALSE	0.2	0.4

A node within a Bayesian network that has multiple parent nodes requires a different NPT. This indicates that the NPT should be elaborated to capture all the relevant possibilities. An example NPT for a node with two parents (and again, Boolean instances) is provided in Table 7.3. The NPT can be further expanded if there are more parent nodes, or more instances in each node.

Table 7.3: Example NPT with two parent nodes

Parent node 1:	**TRUE**		**FALSE**	
Parent node 2:	**TRUE**	**FALSE**	**TRUE**	**FALSE**
Node 3 TRUE	0.9	0.7	0.8	0.6
Node 3 FALSE	0.1	0.3	0.2	0.4

The largest challenge with the NPTs is the estimation of the probability values for each instance. Especially in the case of cyber risks, where the probability estimation is often based on qualitative estimations (as explained in Chapter 3.3.1). Due to the fact that these qualitative estimations could provide an indication of

the plausibility that a certain cyber risk occurs, it is more difficult to estimate an exact probability value for that specific cyber risk.

Applying the cyber risk taxonomy

The scenario- and synthesis idioms, as explained above, are combined into a cyber risk scenario idiom. The synthetic nodes are include to use the elements of the criminal activity theories (Cohen & Felson, 1979; Pfleeger et al., 2015) to estimate the plausibility that the cyber risk scenario will occur. These theories, which are described in Chapter 3.3.1, describe that a criminal activity, such as a cyber risk, will only occur if there is a suitable target, weak defense, and a motivated and capable attacker (Cohen & Felson, 1979). Within the cyber risk taxonomy there are various concepts and variables captured to estimate these three elements. The chosen terminology to indicate these elements is based on Pfleeger et al. (2015) (Motive, Opportunity, and Method). An overview of the graphical structure and qualitative dependencies is provided in Figure 7.4. This structure represents a general cyber risk scenario and could be applied to other cyber risk scenarios. Besides the probabilistic dependency that is displayed with the arrows a qualitative dependency is provided. The qualitative dependencies can either be positive or negative, and are indicated with a plus or a minus.

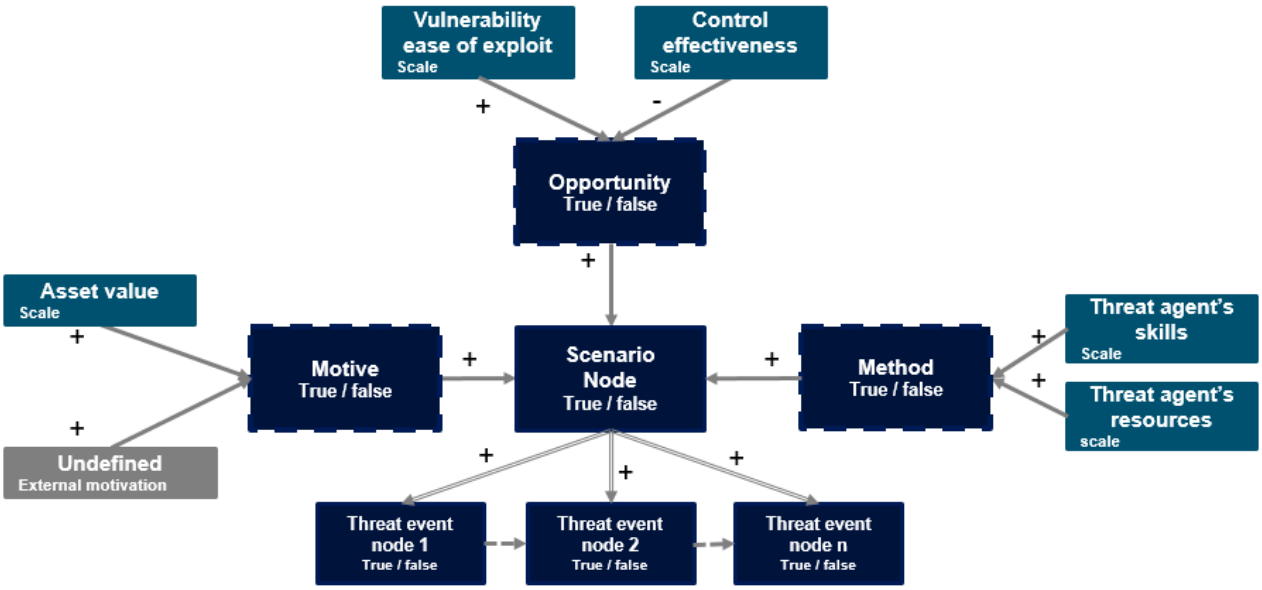

Figure 7.4: Combined synthesis- and scenario idiom to estimate a cyber risk scenario

The nodes in the graph that support the synthetic nodes are based on the taxonomy from Chapter 6, with an exception for the external motivation node (the grey node). This node is captured in the model to indicate that a threat agent, like a script kiddie or hacktivist, could be motivated by something else than the value of the asset he/she is targeting. Although the external motivation node is not captured in a quantifiable manner in the taxonomy. The taxonomy captures, in contrast with the numeric scales for the other nodes, a textual description of the threat agent's motivation. This node will be captured in the Bayesian network as a numeric value. This number provides an indication of the strength of the external motivation, if the threat agent has another motivation to initiate the attack.

The criminal theories, captured with the synthesis idiom, determine the overall plausibility of the cyber risk scenario. The probability values of the threat events within the scenario should be determined separately, but will be influenced by the central scenario node. Assessing the detailed probability values that need to

be entered in the NPT of the network in Figure 7.4 will be a difficult task (Bex & Renooij, 2016; Druzdzel & Van Der Gaag, 2000). Druzdzel and Van Der Gaag indicated that the graphical structure of the network is the most important part. This is due to the fact that the most robust, qualitative, relationships between variables are indicated in this graph. It could therefore be argued that a quantitative graph, such as Bayesian network, is insensitive towards inaccuracies in the detailed numbers. Although there is some evidence that supports this claim, there is not enough evidence for a decisive conclusion for each specific situation (Druzdzel & Van Der Gaag, 2000). Bex and Renooij (2016) indicated the same difficulty during the estimation of all these detailed probability values within a NPT. Within their research they propose a way to translate the qualitative structure towards constraints in a Bayesian network. A similar approach is proposed by Verheij et al. (2016), which includes the translation of qualitative stories towards constraints in the probabilities of a Bayesian network.

The probability values in the cyber scenario Bayesian network are, due to the difficulties with estimating exact probability values to indicate the dependencies, limited to qualitative dependencies. These dependencies indicate if the dependency is either positive or negative, but it does not provide an exact probability value. The probabilistic interpretation of these qualitative dependencies are transferred through the entire network. This indicates that the sub nodes of each synthetic node indirectly influence the threat event nodes via their synthetic node and the central scenario node. The by Bex and Renooij (2016) indicated constraints could be applied to describe the qualitative dependencies. Constraints that are relevant for the graph in Figure 7.4 are as follows: the scenario node will have a low probability if the motive-, opportunity-, and capabilities nodes have a low probability. The second constraint works the other way around and indicates that the scenario node will have a high probability if all three of the synthetic nodes have a high probability. The last constraint is based on the scenario idiom of Vlek et al. (2015) and indicates that the event nodes have a high probability if the scenario node has a high probability. The structure of the NPT of the risk scenario node is provided in Table 7.4. This NPT could be filled with explicit values that are in line with the qualitative dependencies described above. A research to determine these exact values is however outside of the scope of this research.

Table 7.4: NPT of a cyber risk scenario node

Motivation:		**True**				**False**			
Opportunity:		**True**		**False**		**True**		**False**	
Method:		**True**	**False**	**True**	**False**	**True**	**False**	**True**	**False**
Scenario node	**True**								
	False								

The scenario node influences the probability value of each of the threat event below. This dependency is indicated with the NPT that is provided in Table 7.5. The values of the specific threat event node are, besides the scenario node, influenced by their parent event node(s). The specific values within these NPTs should be determined for each combination of threat event nodes. Due to the used idioms the predefined structure of these tables will allow reuse of parts of these tables (Neil et al., 2000). The identification of the exact probability values in the table is, as indicated above, not within the scope of this research. The only probabilistic indication that can be based on this study, is the fact that there is a positive dependency between the scenario node and a threat event node.

Table 7.5: NPT of a threat event node with one parent node

Parent threat event:		**True**	**False**	**True**	**False**
Scenario node:		**True**		**False**	
Threat event	**True**				
	False				

The NPTs of the synthetic nodes are created in a similar matter and their structure is provided in Appendix C. The only difference between these NPTs is the fact that the nodes are not limited to Boolean values. The nodes that construct the synthetic node include categorized scales. The scales are based on the cyber risk taxonomy and rank from 1 to 9. To limit the number of options are the scales categorized in four different categories per node. This categorization, which is included in the taxonomy as well, reduces the number of fields that need to be entered in the NPT from 164 to 32 (the number is calculated by multiplying the number of instances of each parent node with each other, and with the number of instances of the node itself).

CONCLUSION

A Bayesian network can be used to represent the causal structure of the threat events in a cyber risk scenario. The qualitative dependency between the different elements in a cyber risk scenario is indicated in the graphical network, and the detailed probability values are determined with the NPTs. The, in Figure 7.4, captured graph represents the structure of a cyber risk to determine the scenario's overall probability. This structure is a combination between the causal structure of the threat events and a probability estimation of the entire cyber risk scenario in line with criminal theories (as described in Chapter 3.3.1). A combination between these elements allows the estimation of the scenario's (and individual threat event's) probability. These estimations can be further specified in the NPTs. However, these exact estimations require a lot of detailed information about the dependencies, which is often not available. The added value of these exact calculations can therefore be questioned. A similar stance was identified during a validation interview (Chapter 8) and in the research of Druzdzel and Van Der Gaag (2000). There is however not enough evidence resulting from this study and the literature study (Druzdzel & Van Der Gaag, 2000) to draw conclusions about this matter.

The complexity of creating a Bayesian network is, as indicated in Section 7.1, a disadvantage and the reason why these models are not very user friendly. By using idioms as building blocks for the graphical network, the time and effort of creating a Bayesian network can be reduced. This research combines the scenario idiom (Vlek et al., 2015) and the synthesis idiom (as described by Fenton and Neil (2013)). The combination between these idioms resulted in a general overview of a cyber risk scenario within a Bayesian network (Figure 7.4). This structure can be reused to model and estimate a cyber risk scenario to reduce the time and effort. Another advantage of this predefine structure is the ability to reuse both the qualitative graph, and (parts of) the quantified NPTs in new cyber risk scenario models.

7.2.2 CORAS

The model-driven approach to risk analysis within the CORAS consist, in contrast with ANRAM and Bayesian networks, of both a modeling language and a risk analysis method. This section describes the CORAS method and how this could be combined with the cyber scenario taxonomy. This is followed by a description of the CORAS modeling language and the possibility to include cyber scenario specific elements within a CORAS model.

CORAS METHOD

The CORAS risk method contains eight steps that should be followed to identify, asses, and treat potential risks within your organization. These steps, which are presented in Figure 7.5, include the identification of the asset at risk, the potential threat diagrams, and the possible ways to control the risk in treatment diagrams. The remainder of this section will not describe all the steps in detail, but will focus on the overall method.

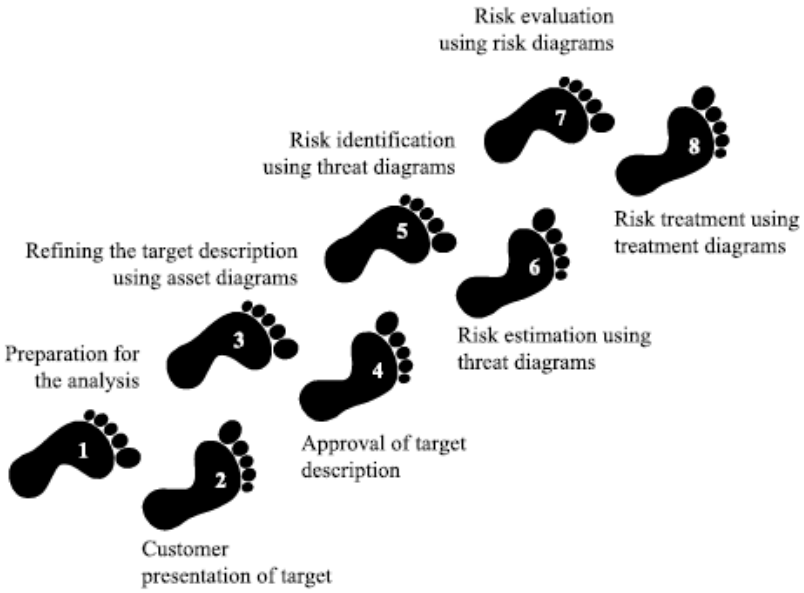

Figure 7.5: The eight steps of the CORAS method (Lund et al., 2010)

The objective of the third step is the finalization of the asset diagrams to represent the asset at risk. The asset diagrams describe the most important assets that are targeted by potential threat agents. Besides the asset themselves, their relations to other important assets are included. These relations could indicate which assets are harmed once the central asset is compromised (e.g. the public's trust in a service after a major data breach that included personally identifiable information). This step provides more information about the context of the asset, which includes the information that is needed in the taxonomy of Chapter 6.

The targeted assets that are identified form the end goals in the threat diagrams that are created in step five. This step includes a workshop to identify as may potential unwanted incidents as possible. These incidents include vulnerabilities, threats, and threat scenarios. Within the CORAS methods these incidents are modeled in the CORAS language. The concepts and variables of the taxonomy guide this process by providing the needed information to identify a complete story, and to allow the analyst to document relevant contextual information in a structured manner to complement the threat diagrams.

The in step five identified threat diagrams do not include the likelihood and consequence estimations. The CORAS method includes qualitative pre-defined scales. The definition of the values of these scales should be tailored towards the specific situation by performing brainstorm sessions with experts and analysts. Qualitative related scales could be used to indicate the likelihood and consequence of a threat scenario. They proposed the following scale for the likelihood: unlikely, possible, likely, certain. For the consequences they proposed: insignificant, minor, moderate, major, and catastrophic. The qualitative scale that represent the consequence could be combined with the business impact estimations of the taxonomy by providing a

combined consequence estimation of the financial, reputational, and non-compliance impact. The likelihood estimations should be based on the attractiveness of the asset (motivation of the threat agent), capabilities of the threat agent (method), and the presence of vulnerabilities (opportunity), as explained in 3.3.1.

The final step within the CORAS method is the identification of suitable controls to reduce the impact or likelihood of a risk scenario. The treatment diagrams should be added within the scenario models to indicate at which point in the scenario will be affected. Within the CORAS method the impact of a treatment scenario on the rest of the scenario is not explicitly mentioned. This impact could be mentioned with the taxonomy since a treatment scenario will reduce the vulnerabilities (and therefore the likelihood) or the business impact of an occurred incident.

CORAS MODELING LANGUAGE

The icons in the CORAS modeling language are created to provide a clear overview of the different elements within a security risk scenario. These icons capture the likelihood estimations of the threat scenarios, unwanted incidents, and the relation between these elements. The likelihood values are divided over five different scales and indicated with qualitative values leading from certain towards rare. The impact values are added to the relation that an unwanted incident towards a certain asset. There are again five different scales proposed, which lead from catastrophic towards insignificant. The meaning of those scales will however differ per situation (as indicated above), it is therefore part of the CORAS method to determine these values (Lund et al., 2010). An overview of the symbols within the CORAS modeling language together with the likelihood and impact scales is provided in Appendix D.

The cyber risk scenario in Figure 7.6 is based on the CORAS modeling language, likelihood and impact, estimations, and the general steps within the CORAS method. The information about this scenario is gathered from the Deloitte risk repository. The focus of the modeled scenario should be on the causal structure of the threat events. The proposed impact and likelihood estimations are rough estimations given the limited amount of context that was provided with the scenario.

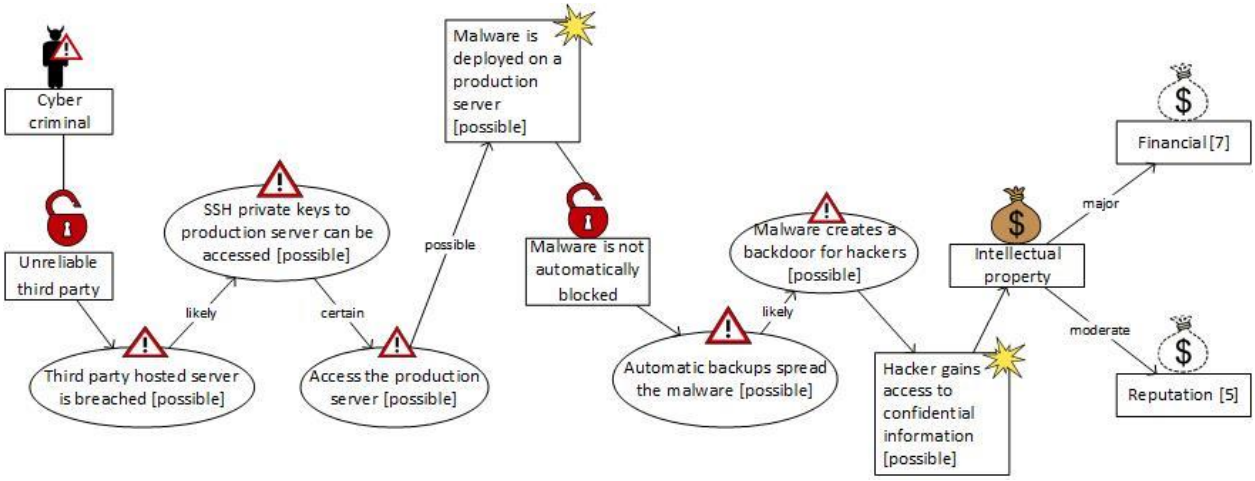

Figure 7.6: An example cyber risk scenario within the CORAS model

One of the main purposes of a CORAS scenario model, like the model in Figure 7.6, is to support the communication and interaction between the different stakeholders that are involved (Braber et al., 2007). This use, together with the possibility to provide qualitative based impact and likelihood estimations, provides a useful model to complement the detailed information that is captured within the taxonomy. A

disadvantage of the CORAS model is the lack of formal propagation rules between the likelihood and impact estimations. The likelihood values in Figure 7.6 indicate the likelihood of a certain relation between two events, or the likelihood that a specific event occurs in the context of the entire scenario. Besides the likelihood values, which is primarily used in the CORAS models, it is possible to indicate the chance that a certain event occurs with a probability estimation as well. The probability estimations will be translated to comparable qualitative scales.

The impact estimations within CORAS can be elaborated with the business impact estimation of the cyber risk taxonomy. By modeling the different elements that determine business impact as indirect assets, the scenario is provided with an impact estimation that is both understandable for technical oriented stakeholders (the direct assets) and business oriented stakeholders (the indirect assets). Figure 7.6 therefore contains both the CORAS impact estimation, captured within the relation, and the business impact estimation of the taxonomy within the indirect assets.

Conclusion

The focus of the CORAS risk models within the CORAS method is to provide an easy and understandable overview of the cyber risk scenario. This overview is provided by the relatable icons that are used in the model. These icons provide a good overview of the relevant elements within a security risk. Due the overlap in the context of the CORAS model and cyber risk it is possible to apply this model to visualize the causal structure of cyber risk scenarios. Another advantage of the model is its user friendliness, due to the qualitative basis of the model.

Although the main purpose of the CORAS model is to provide a qualitative overview of the risk scenario, it is possible to provide likelihood and impact indicators in the model. Both of these values are based on predefined qualitative scales. These predefined scales consist of domain specific values, which should be tailored for each specific risk. The impact estimation of cyber risk scenarios could use the impact scales that are determined in the taxonomy of Chapter 6 to express the impact of the cyber risk scenario.

7.2.3 ANRAM

ANRAM models describe the story of a risk via structured, semi-formal scenario schemes. The different concepts within those scenario schemes are arguments, which are structured via argumentation schemes. These argumentation schemes consist of three different types of arguments: claims, risk factors, and controls. Based on these scenario schemes, and the underlying arguments, a structured story of the risk is provided.

Developing scenario schemes

A scenario scheme within ANRAM should consist of six different elements (Hovestad & Bex, 2016). These elements describe the core concepts within the risk scenario. These different elements, together with a description and the application within the cyber risk taxonomy, are provided in Table 7.6 below.

Table 7.6: Elements within a scenario scheme

Element	Description	Application in cyber scenario
The risk that the scheme explains	The risk that the scheme explains is the main risk event of the risk scenario.	This risk indicates the action that causes the business impact.
Central action of the scheme	In a scenario, the events are connected through causal links. The central	The central action within the scheme is described by the different threat

	actions of the scheme are the events directly connected to the main event.	events that a threat agent should perform in order to reach his goal.
Relevant risk factors	Relevant risk factors can be recorded in a scenario scheme.	Relevant risk factors include known vulnerabilities within the IT landscape (both social and technical).
Relevant controls	In addition, relevant controls can be made explicit.	Relevant security measures that are implemented could be added.
Relevant information	All relevant information that could affect the risk scenario.	Contextual information about the targeted organization, and the asset.
Pattern of actions	Patterns of action show how the risk factors are connected.	Defines the flow between the threat events.

The concepts within the taxonomy of Chapter 6 have some differences and overlap with the elements in the scenario schemes. The main overlap lies in the identification of the different events that eventually lead to the risk. A difference between the cyber risk taxonomy and ANRAM is caused by the different focus of the risk scenarios. The focus of ANRAM is fairly broad, and not necessarily focused towards risks of a specific 'asset/target' of a 'victim'. Since these elements (the target of an attacker and a victim that is targeted) are crucial within a cyber risk scenario, it should be added within the scenario schemes.

Arguments in ANRAM

The arguments within a scenario are one of the main concepts within ANRAM. These arguments are used to attack or support the elements and relations within the scenario. An argument-based approach, like ANRAM, uses arguments and counterarguments to expose sources of doubt in the reasoning and therefore provides a justified conclusion (Bex, 2011). Within ANRAM are four different kind of arguments included: risk factors (orange boxes in the model) that increase the risk within the scenario, controls (green boxes in the model) that decrease the risk within the scenario, and claims (grey boxes in the model) and evidence (purple boxes in the model) that could support or attack risk factors and controls in the scenario.

Assessing the scenarios and arguments

Each argument receives both a plausibility (P) and impact (I) value. These values indicate the chance and the impact that the argument contains. These values are propagated from one argument to another via a fixed set of rules (Bex & Hovestad, 2016). These rules explain what happens with the P value if one or more arguments support or attack a certain conclusion (or other arguments). The supporting rules indicate that evidence, risk factors, or claims will propagate their P- and I value directly to their conclusions. If multiple arguments support a conclusion, the highest I value is propagated, and in case of an OR, or XOR joint, the highest P value as well. Only if the join of these arguments is via an AND statement, the lowest P value is propagated. An overview of the complete set of propagation rules, together with an indication of the used scales, is provided in Appendix E.

A scenario has, just like the individual arguments, a P- and I value. These values are determined by the sum of the values of the arguments within the scenario. This sum only takes the 'undefeated' arguments, within the scenario, into account. An argument can defeat another argument if the arguments attacks another argument with a lower plausibility value. It is important to note that a defeated argument cannot attack or support another argument.

APPLYING THE CYBER RISK TAXONOMY

As explained above ANRAM is applicable to a broad range of risk scenarios. The core structure is therefore applicable to model cyber risk scenarios as well. There are however a few differences between ANRAM and the cyber risk taxonomy. The biggest difference is the fact that cyber risks require an attack-based assessment, where ANRAM is focused towards general risk events without a clear attacker (threat agent), or target (asset), which play an important role within a cyber risk scenario. These elements could be incorporated within the claim statements of ANRAM. Another option to incorporate these elements, is the introduction of new arguments within ANRAM. To keep the argumentative-narrative approach of ANRAM (Bex & Hovestad, 2016) this research incorporates these elements within the claim-arguments. An advantage of these claims is the possibility to infer generalizations from the claims that are often proposed. The three different claims are described and elaborated with an example in Table 7.7.

Table 7.7: Attack scenario specific claims

Claim	Description	Examples
THREAT AGENT	Claims about the threat agents include indication about their skill level, as well as their resources. Claims about probable threat events could be included as well (as described in Chapter 5.4).	The use of phishing mails is often used as a starting point of a cyber risk. State oriented threat agents are technical skilled and got the resources to perform a sophisticated cyber risk.
ASSET	Claims about the asset indicate its value towards the targeted organization as well as towards the attacker. These claims could increase the plausibility of an attack.	Personally identifiable data is valuable towards attackers to perform fraudulent activities. Data breaches that include client information cause reputational damage.

Once the above mentioned elements are made explicit within the model ANRAM provides a good and understanding overview of the patterns of threat events within the scenario. This overview is strengthened with the P- and I value as well as the propagation rules (described in the previous sub section). A limitation of the current ANRAM risk assessment model and the cyber risk taxonomy is the lack of contextual information that could be incorporated in the model.

Based on the ANRAM model we have created a cyber risk scenario (captured from the cyber case repository of Deloitte). This model describes the cyber risk scenario where a threat agent exploits a zero-day vulnerability (an undisclosed and previous unknown vulnerability in an IT system) to gain access to the organization's source code repository. Besides the risk factors that represent the threat events, includes the model claims about the attacked asset, the way it was attacked, and the attacker. The interplay of these arguments in the scenario is captured in Figure 7.7.

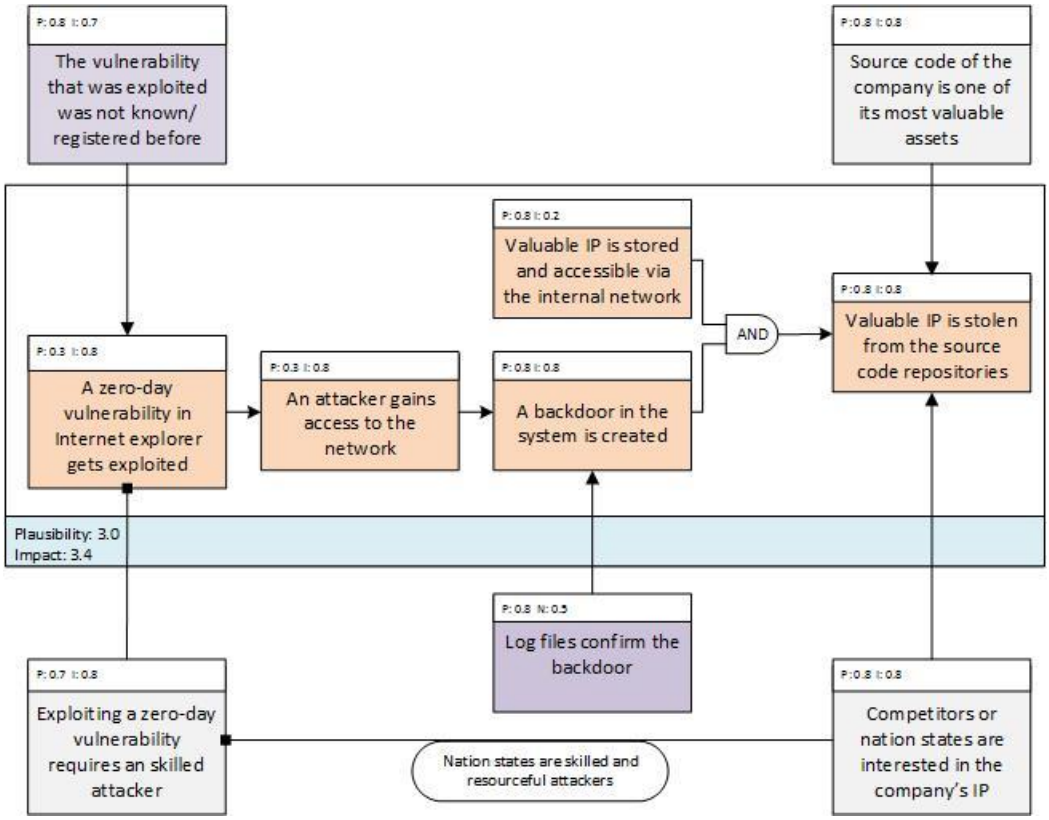

Figure 7.7: An ANRAM of a cyber risk scenario

CONCLUSION

ANRAM provides a general applicable understandable overview of the different risk factors, claims, evidence, and controls within a risk scenario. This structure allows the creators of the risk scenario to visualize the pattern of action of the different risk factors and elaborate this structure with claims, evidence, and controls to attack or support the risks. Another advantage of ANRAM is the formal, logical grounding which determines the overall impact and plausibility values of the scenario. Another advantage of the model is the possibility to explicitly infer or capture generalizations in the scenario. Because these generalizations are explicitly mentioned it is possible to reuse them in other risk scenarios.

Besides the advantages there are some difficulties with ANRAM that we encountered during the modeling of a cyber risk scenario that was in line with the taxonomy of Chapter 6. The main difference between the cyber risk scenarios and the scenario- and argument structure of ANRAM is, as indicated above, the lack of a threat agent and targeted asset. These elements can, as demonstrated in Figure 7.7, be incorporated in the claim arguments of ANRAM. A disadvantage of this combination is the loss of the specific characteristics of these elements.

A last difficulty that we encountered with ANRAM were the arguments that attack another argument. In the current logical model, it is only able to completely defeat another argument. In the case of the cyber risk scenarios, it is often the case that a claim, or piece of evidence, will reduce the plausibility of a risk, but that does not indicate that it becomes impossible for that risk to occur. It should therefore be more appropriate to include arguments that increase, or decrease a certain risk factor in the scenario. A disadvantage of a more precise estimation of the influences is the added complexity and necessary information to determine

these values. It is therefore necessary to align the needs of the model together with the available information to determine the values and the level of detail that will be used in the modeling.

7.3 USING A CYBER RISK SCENARIO MODEL

This section will describe the different ways in which the cyber risk model can be used. Three different ways in which such a model could be used are identified: cyber risk investigation, cyber risk knowledge sharing, and cyber risk analysis.

7.3.1 CYBER RISK INCIDENT INVESTIGATION

A predefined structure of a general cyber risk scenario could help with an investigation towards an occurred cyber incident. An investigation towards an occurred cyber incident is usually based on the log files of the systems that were compromised. These files do not always provide a complete overview of what happened. By combining the information of these files with earlier created models, it is possible to identify the missing information from the log files. This use however requires a large set of modeled cyber risk scenarios in order to match the occurred incident with a predefined scenario. One way to increase the amount of risk scenarios that an organization can use is to share these scenarios with other organizations. The following Section elaborates on this use.

7.3.2 CYBER RISK SCENARIO KNOWLEDGE SHARING

As indicated in Chapter 3.1.4, knowledge sharing about cyber risk scenarios is a valuable source to gain more knowledge of relevant threats in the cyber threat landscape. An initiative of the NCSC (the Dutch Center of Cyber Security) to support the sharing of such knowledge resulted into the introduction of ISACs (Nationaal Cyber Security Centrum, 2015). ISACs are a collaboration between the government and several organizations that meet between two and eight times per year to share their experiences with occurred and prevented cyber risks. These meetings provide useful information of cyber threats, but this source of information is limited to the meetings. If the modeled cyber risks are shared in a uniform and structured manner (which is possible with the cyber risk models) it could result into a useful and powerful source of information towards an organization.

There are some initiatives that support the sharing of such scenarios (e.g. TAXII (Davidson & Schmidt, 2014) or CDXI (Dandurand & Serrano, 2013) which are described in Chapter 3.1.4). These initiatives are however not broadly accepted and used in the field. This is mainly due to a resistance for sharing such knowledge. An occurred cyber threat that is reported could for instance result into reputational damage (Choo, 2011). Another disadvantage is that a shared scenario can function as a ‘playbook’ for an attacker that represents vulnerabilities of a certain organization. It is therefore important that the shared information remains confidential and secure.

7.3.3 PROACTIVE CYBER RISK ANALYSIS

Besides modeling and sharing cyber risk related incidents, it is possible to use a cyber risk model to perform, or elaborate, a cyber risk analysis. Such an analysis will start with the identification of potential cyber risk scenarios as described in Chapter 6.2. The causal structure of the cyber risk scenarios can be used to identify where the organization should apply certain cyber security controls in order reduce the probability of such a cyber risk. The estimation of such a probability (or plausibility) value is possible once the scenario is applied to one of the causal models. Even a qualitative model (such as CORAS) provides an indication of the chance that a certain cyber risk scenario causes a certain impact. These estimations can, with enough information about the probability values in a cyber risk, be further specified in a more quantitative model (such as

Bayesian networks). These estimations can be calculated with, and without, a certain cyber security measure and they therefore provide an overview of the effectiveness of the applied cyber security measure.

A cyber risk scenario, which is modeled in a more qualitative model, can provide a valuable and understandable overview of the potential scenario. During the validation interviews it was indicated that such an overview of the risks and the consequences would be valuable to use in the internal communication. Such an overview can convince an organization of the concerns of potential cyber risks. A model that is used for this purpose should be focused towards the qualitative structure of the high level threat events and consequences, instead of a detailed technical scenario or a scenario that provides a complex probability estimation.

7.4 CONCLUSION

This chapter described the application of the cyber risk taxonomy within a causal model. The models that were used included quantitative as well as qualitative causal models. They were used to capture the causal structure and estimate a probability or plausibility value to indicate the chance that such a scenario would occur. In total there were three models used that range from a quantitative (Bayesian networks), a semi quantitative (ANRAM), to a qualitative model (CORAS).

A disadvantage of the quantitative Bayesian networks was the effort and necessary detailed information to construct the model. Although the effort could be limited by introducing idioms as building blocks for the network, remained the needed information a limitation of the Bayesian network. Given the limited amount of structured cyber risk information, it remains difficult to determine reliable values within a node probability table (NPT). ANRAM requires, in contrast with a Bayesian network, less detailed information. Although the scenario's overall estimation is based on a formal logical grounding, the plausibility and impact estimation of the individual arguments is based on assumptions. These assumptions can be supported, or attacked, with other arguments to improve its reliability. The main advantage of CORAS model is that the model is understandable, and could be created without a lot of effort. This model is therefore very suited for the visualization and communication of cyber risk scenarios. A disadvantage of such a model is the lack of formal rules to estimate probability or impact estimations in the model. This disadvantage is however partly solved with the CORAS method, which guides a user with the scenario identification and estimation phases.

Both the qualitative (CORAS) and quantitative (Bayesian networks and ANRAM) were able to capture the cyber risk scenario from the taxonomy in Chapter 6. A choice between these different models should therefore be based on the needed level of detail of the modeled risk. If the user would like an understandable, and quick overview of the cyber risk scenario, a CORAS model would be the best fit. But if a user would like to provide a more elaborate probability estimation to further analyze possible cyber risk scenarios, and the user has a lot of detailed (and quantified) information about the scenario a Bayesian network should be selected. The ANRAM model requires less detailed information, but provides a clear overview of the scenario's elements and the overall plausibility and impact. During the selection phase of a specific modeling language should, besides needed level of detail of the output, the level of detail of the available information be taken into account. This is due to the fact that the output of an exact and complex calculation with 'unreliable' data remains 'unreliable'. There is however not enough evidence provided in this study to conclude the above mentioned statement.

The final part of this chapter described the three different ways in which a cyber risk scenario model can be used. A distinction between proactive and reactive uses could be made. The reactive ways to use these

models include the modeling of occurred cyber incidents to identify the vulnerabilities that allowed the risk to occur. Another way to use the structure, modeled, cyber risk scenarios, is to share them with other organizations. The shared scenarios form a valuable source for organizations during the risk identification phase of a risk analysis method. The proactive way in which a scenario model could be used is within the risk description and estimation phase of a risk analysis method. Where qualitative models provide a good and clear description of a risk scenario to communicate the potential risks, quantitative models provide the ability to perform probability and/or impact estimations of the cyber risk scenario.

8. RESEARCH VALIDATION

The cyber risk taxonomy was identified and constructed by conducting a literature review and expanded with the cyber risk practices and knowledge within Deloitte. The knowledge from within Deloitte was gathered via unstructured several interviews from both technical- as business experts in the field of cyber risks. The findings of these interviews resulted in new ideas and literature sources. In order to use these ideas in our research a literature review was conducted to confirm the ideas and findings. To validate the findings that were used within the taxonomy we performed six validation interviews with cyber security experts from different organizations. These validation interviews were aimed at the business application of the proposed taxonomy, and therefore the social relevance cycle of Hevner (2007). Besides the validation interviews, cyber incidents from the Deloitte cyber risk repository were gathered to validate the completeness of the taxonomy in order to capture incidents from the real world. Both of these validation approaches together with their findings and implications are described in the sections below.

8.1 VALIDATION INTERVIEW PROTOCOL

The goal of the validation interviews was, as described above, to validate the possible applications of the proposed taxonomy towards the needs from the organizations. This included a discussion about the key drivers for an organization to choose such an approach, as well as to share the cyber risk knowledge with other organizations. This goal was achieved by conducting semi-structured validation interviews with six different cyber security experts of six different organizations. The interviews were started with a short explanation of this research and its preliminary theoretical findings, and followed with several open questions towards the expert. These questions were aimed at the current, and desired, situation of the organization, the possible applications of cyber risk scenarios within the organization, and the advantages and disadvantages of sharing information about occurred cyber risks with other organizations. An overview of the validation protocol, which includes the questions, is provided in Appendix F. The function of each of the interviewed expert is provided in Table 8.1. Each of the interviews worked in an IT security related function of a different organization. Two of the interviewed experts were Deloitte employees who worked intensively for a single client organization in a cyber security related project and function. The interview was therefore aimed towards their situation at the specific client.

Table 8.1: Functions of the interviewed experts

Expert	Function
Expert 1	Global Security Officer
Expert 2	Security Officer
Expert 3	Senior manager Deloitte – Cyber security project lead
Expert 4	Senior manager Deloitte - Interim CISO
Expert 5	Cyber Security Manager
Expert 6	Information Security Manager

8.1.1 INTERVIEW SESSIONS

Six validation interviews with six different cyber security experts were conducted. The interviews were semi-structured and included open-ended questions. These questions allowed us to identify new and relevant topics that were addressed during the interview itself. An advantage of the semi-structured interviews over unstructured interviews was the ability to better prepare ourselves with a set of predefined questions. After the interviews were conducted there were summaries created of these interviews. The summaries were based on the notes we took during the interview and, if available, the recordings we made (the recordings were only made after an agreement with the interviewed expert). These summaries were created within 24 hours after the interview and were structured per question/subject that was addressed within the interview. After the summaries per interview were created, a central overview of all the findings of the interview was created. For each finding we kept track of the number of experts that indicated the finding.

8.1.2 INTERVIEW RESULTS

The validation interviews resulted into several findings about the practical applicability of our research. The different findings are summarized in this section. The findings are gathered from summaries that were made of the different validation interviews and are divided between the different aspects of the validation interview: scenario based risk analysis approach, the cyber risk taxonomy, and cyber risk knowledge sharing. An overview of the different findings during these validation interviews is provided in Table 8.2. Besides the findings is indicated how many of the different experts mentioned the finding. This however does not indicate that the remaining experts did not agree with the finding. This is due to the fact that we did not specifically asked the experts towards these findings and thus the experts mentioned these topics by themselves. Only the findings that were mentioned by at least two different experts are captured in Table 8.2. The table divides the different findings over three different topics and provides a short description. The elaborate descriptions of the findings, include a description of the possible application of the specific finding.

Table 8.2: Validation interview results

Topic	Finding	Total
Using the risk scenarios	Scenarios could be used to communicate the consequences and impact of potential risks	5
	The current organization lacks a structure to create such scenarios	3
Scenario based risk analysis	A risk scenario needs context to identify if your organization is at risk for such a scenario	5
	Scenario could be used to elaborate the risk analysis approach	5
	Scenario needs a clear overview of the IT landscape, which could be a problem	3
	The scenario based approach could result into an overload of potential risk scenarios	2
	Identifying and constructing the scenarios would be very time consuming	2
Cyber risk knowledge sharing	Current knowledge sharing approaches are unstructured	3

	Knowledge sharing would require an independent platform (third party) to rearrange it (e.g. like the ISACs)	3
	A win-win situation needs to be created in order to make facilitate the knowledge sharing	2

USING A CYBER RISK SCENARIO

One of the valuable uses of the cyber risk scenarios that was identified during the validation interviews, was indicated by five of the interviewed experts. They indicated that the scenarios are a valuable tool to communicate the risk internally towards for instance the board. The scenarios provide a good overview of the possible consequences if certain security measure are (or are not) taken into account. A scenario that is used to communicate a risk with the board should be more high level and focused towards the potential caused business impact over the technical details of the risk.

All of the experts indicated that it would be possible to create and use the scenarios in a cyber risk analysis approach. Three of the organizations already performed comparable approaches to include risk scenarios within the risk analysis. They however did not use a structured method or approach to construct these scenarios. One of the experts indicated that they used their knowledge and experience to create these scenarios, but they were looking for one specific structure, or language, to capture the identified scenarios. He indicated that the, by this research proposed, taxonomy could be a possible solution for their need.

SCENARIO BASED RISK ANALYSIS

Five of the interviewed experts indicated that it is important to use a scenario based risk analysis to elaborate a more standardized threat-, or vulnerability based risk analysis. An expert indicated that the standardized security measures (e.g. complying with an ISO or NIST standard, deploying up to date firewalls, patching the systems and applications) would stop the majority of the threat agents and provide a basic level of security. These measures would however not stop the advanced persistent threats towards the most valuable assets of an organization. A scenario based risk analysis is able to identify, and control, these threats. Given the needed effort to perform a scenario based risk analysis they indicated that an organization should identify their most valuable assets (that are vulnerable towards cyber threats), and perform a scenario based risk analysis towards these specific assets. The creation of cyber risk scenarios would be a valuable approach to identify and control these threats. It is therefore needed to combine both approaches, provide a basis security with more standardized vulnerability or threat based approaches, and perform a deeper analysis towards the most valuable assets.

Three of the experts identified a potential problem during the creation of the cyber risk scenarios. This problem is caused by the needed information about the IT landscape of the organization. Since a scenario includes multiple applications and systems, it is needed to have an overview and the dependencies of all of these systems and applications as well. Most organizations have some enterprise architectures or documentations of their IT landscape, these architectures are however often not up-to-date with all the details of the organization's current situation. It is therefore important to be aware of this, and not to completely rely on these documents. The system- or application owners could, and maybe should, therefore be included in the risk analysis approach.

Two other limitations towards the scenario based risk analysis that were identified include the large amount of possible risk scenarios and the needed effort to construct a cyber risk scenario. Both of these limitations are however already indicated above. It was mentioned that the scenario based analysis should be used to

elaborate a standardized risk analysis. This will reduce the number of risks that should be translated towards risk scenarios. It however still takes a lot of effort to create the scenarios and it is therefore important to identify the most valuable assets (which could cause the largest business impact towards the organization) and only perform a scenario based risk analysis towards these assets.

The experts indicated that the concepts in the taxonomy provided a good overview of a cyber risk scenario. But it is important to note that the taxonomy's variables were not discussed in detail during the interviews. One of the experts indicated that it is important for the taxonomy to be adaptable to a specific organization, as well as to the development of the cyber threat landscape. The interviews did not result into new concepts that should be captured within the taxonomy. However, as indicated above, the taxonomy's concepts were, due to time limitations in the validation interviews, not discussed in detail during the interviews.

CYBER RISK RELATED KNOWLEDGE SHARING

The experts indicated that there is a need towards the sharing of cyber risks. There is currently a limited amount of knowledge shared and the knowledge that is shared is often unstructured. One way in which the knowledge was shared was via the ISAC's of the Dutch Cyber Security Center (Nationaal Cyber Security Centrum, 2015). An advantage of an ISAC is the confidential setting in which the knowledge is shared. This is needed since a cyber incident indicates certain vulnerabilities of the organization as well. Another example was provided by one of the experts where the law enforcement contacted the organization about a potential threat. Organized cyber threat agents attacked a comparable organization and would most likely use a similar approach towards their organization. This was however the only concrete example of cyber risk knowledge sharing to prevent a potential cyber risk that he could remember, which both illustrates the added value of sharing such knowledge and the limited amount of cyber risk knowledge that is currently being shared.

Two of the experts indicated that, in order for the knowledge sharing to be successful, it is necessary that a third party would arrange the sharing of the cyber risk scenarios. This third part should arrange the distribution of the scenarios, as well as sanitizing them were needed. Besides the third party, it was indicated that a win-win situation was needed for the knowledge sharing to be successful. This situation could be achieved by arranging a good balance between the effort it takes to share the knowledge and the added value of the received scenarios.

8.2 DATA VALIDATION

The information within the Deloitte cyber case repository is, as described in Chapter 2.1.3, used to assess the proposed cyber scenario taxonomy. Capturing the cases within the repository allowed us to assess the ability of the taxonomy to capture real cyber incidents. This validation session was performed within an Excel file. For each concept in the taxonomy an Excel sheet was created that contained columns with the different variables. Via the ScenarioID that was provided for each concept it was possible to keep track of the complete scenario. In total there were 40 different risk scenarios (that included 151 threat events) captured in the Excel sheet. A disadvantage that was encountered with the Excel sheet was the lack of an understandable overview of the risk scenarios. The lacking overview of the entire scenarios was partly the result of the large amount of variables in the taxonomy. The dependencies between the different concepts in the taxonomy was not explicitly captured in the Excel sheet as well as the taxonomy. These dependencies, especially between the different threat events, provide valuable insights towards an organization. These two findings therefore strengthened the need for a causal risk model to capture these dependencies and provide a clear overview of the scenario. The risk model should be used to complement the taxonomy.

Besides the overall finding about the lack of an understandable overview in the Excel sheets, there were some findings about the cyber risk taxonomy itself. Five findings, together with their implication, are provided in Table 8.3. The implication column in the table describes if the finding resulted into changes in the taxonomy, or if the finding requires further research.

Table 8.3: Findings after the data validation

No	Finding	Implication
1	The taxonomy is able to capture real cyber incidents; it is however sometimes quite detailed which makes it difficult.	No variables were added after the data validation. It could however be needed to further evaluate the taxonomy on his level of detail.
2	The level of detail in the sheet has a negative influence of the readability of the scenarios.	The structure of the concepts was addressed during the validation interviews. The individual variables were, due to time constraints, not validated. More detailed validation sessions could help with the identifying the relevance of each variable.
3	The identified threat events in a risk scenario were difficult to categorize in the predefined threat categories.	This finding was partly caused by the lacking detail in the descriptions of the cyber incident. The used risk categorization provided more detail, as well as examples. The feasibility of organizations to use the categorization could be further investigated.
4	The causal structure between the events is difficult to determine/visualize in the current taxonomy.	The causal structure is needed to identify the events in the scenario that could best be controlled. The overview of this structure is specified within the cyber risk scenario models of Chapter 7.
5	Threat events within a cyber risk scenarios are executed in an unstructured order	The taxonomy did not restrict a predefined order of threat events within a cyber risk scenario, as this was already described in Chapter 5.5.2. It was therefore not needed to adjust the taxonomy.

9. CONCLUSIONS

The objective of the conducted research was to identify an approach to capture cyber risk scenarios in a structured manner. The scenarios should be usable in a cyber risk analysis and, due to the structure, allow for reuse in future risk analyses. This objective was based on the research's problem statement. The problem statement is summarized below.

The cyber threat landscape is growing in both its size as its sophistication. These sophisticated cyber threats are often targeted towards one target and consist of multiple threat events. In contrast with these multi-staged attacks, the majority of the risk analysis approaches is still focused towards 'atomic' threats (Barnum, 2014). Besides the needed focus towards risk scenarios over atomic risks, it is necessary to capture this knowledge in a structured manner to allow reuse and the creation of an organizational memory (Nonaka, 1994). Most risk analysis approaches result into valuable insights, but since the results are often unstructured and based on the experience of the analysts it is difficult to reuse this information in a new situation.

The proposed cyber risk taxonomy and cyber risk scenario model provide the needed structure to capture entire risk scenarios for analysis and knowledge sharing purposes. This chapter summarizes the research findings that provide answers to all of the sub questions of this research. Based on these different findings a final conclusion is drawn. This conclusion provides the answer to the main question in this research, which is based on the research objective described above.

9.1 CONCLUSIONS OF THE SUB RESEARCH QUESTIONS

The answer of the main research question is divided over the seven sub research questions. This section provides the answers these seven sub research questions.

1. **Which steps and approaches are performed within a risk analysis?**

A general risk analysis approach follows three steps: identify, describe and estimate. There are several methods and approaches that provide more detailed instructions to take these three steps. The risk identification step of a risk analysis could be achieved via three different approaches: a threat-, an asset-, or a vulnerability based approach. Pfleeger et al. (2015) indicated that a combination between all three of those approaches is needed to identify all the potential risks towards an organization. The objective of the second step, describing a risk, is to describe the identified risks together with the needed context in a structured format. These descriptions simultaneously check if the identification phase was comprehensive enough and prepares the analyst for the risk estimation step. The risk estimations are often focused towards the probability that the risk occurs and the impact that could result from the risk. The approaches to estimate these values range from mathematic quantitative measures to more qualitative estimations. A quantitative approach should be used if a detailed and exact risk estimation is needed. Quantitative- in contrast with qualitative approaches however require exact, and detailed, input values to perform the calculation. A choice between these approaches therefore depends on the needed level of detail of the risk estimation, as well as the available information to perform the calculation or estimation.

2. What are the different concepts within a risk scenario?

Different descriptions, with varying levels of detail, of a risk scenarios exist. A more general and high level risk scenario can be described as the interplay between a certain trigger that allows a risk event to occur, which causes a potential consequence (Fenton & Neil, 2013). This research identified various risk scenario models and descriptions. The identified models resulted into the seven different concepts that should be captured within a risk scenario, as described in Chapter 4.2. These scenario concepts were further elaborated to capture the contextual elements of a risk, as well as the needed cyber aspects of a risk in Chapter 6. These contributions were based on the research of De Kock (2014) and the STIX framework (Barnum, 2014). This combination resulted into the following concepts to capture the entire story of a cyber risk scenario:

- General scenario information
- Organization (victim)
- Threat agent (attacker)
- Asset (target of the attacker)
- Threat event (multiple events possible)
- Business impact
- Vulnerabilities
- Controls

Table 6.1 provides an overview of these different concepts together with their reference with De Kock (2014), the STIX framework, and/or the in Chapter 4.2 identified risk concepts.

3. What are possible probability and impact estimations within cyber risk scenarios?

Impact and probability estimations are often used to indicate a risk value (Fenton & Neil, 2013). The resulting risk values could be used to prioritize the different identified risks. As indicated in the answer of the first sub research question, a distinction between quantitative and qualitative estimation approaches exist. Both of these approaches are used in the estimation of probability and impact values for a cyber risk. Suh and Han (2003) proposed a method to calculate the potential impact of a cyber risk in terms of the losses in monetary values due to the risk. This calculation is based on the direct costs (e.g. the replacement costs of a harmed computer) and the indirect costs (e.g. a disrupted business process due to a denial of service attack). It is indicated that the biggest financial impact of a cyber risk is caused by the disruption of the business (Ponemon Institute, 2015; Suh & Han, 2003). Besides the financial aspect the reputational and regulatory impact of a cyber risk should be taken into account as well. These two aspects are, like the indirect costs, difficult to quantify. It is therefore useful to use structured scales to determine the reputational and regulatory impact (OWASP, 2015a).

Three different approaches to estimate the probability of a risk can be identified: the traditional-, the frequentist-, and the subjective approach. The traditional approach to calculate the chance that a risk occurs requires a fixed set of possible stages, as well as a known set of stages in which the threat occurs. The frequentist approach calculates the chance of an incident in a similar matter. The approach is applicable to situations that could be repeated under the same conditions (e.g. rolling a dice). The chance of a risk is then based on the number of occurred incidents, divided by the total number of occurred events. Both of these estimation approaches are difficult to use to estimate the probability of a cyber risk. This is mainly due to the lack of (historic) data to perform these calculations (Byres & Lowe, 2004). With the subjective approach, it is possible to estimate to probability that a certain risk occurs without a large set of structured historical

data. The probability value is based on the predefined probabilistic dependencies between certain elements. The combination of these elements estimate the chance that a certain incident occurs. This approach is applied in the criminal theories of Cohen and Felson (1979) and states that a criminal act, like a cyber risk, can only occur if there is a motivated attacker, weak defense, and a suitable target. The criminal theory is proven to be applicable within the cyber security context (Byres & Lowe, 2004; Choo, 2011; Pfleeger et al., 2015). We can therefore conclude that the probability of a cyber risk is dependent on the resources and skills of the threat agent, vulnerabilities in the organizations IT security, and the value of the targeted asset. The influence of these elements towards a cyber risk remains qualitative and therefore only indicates if there is a positive or negative probabilistic dependency.

4. **What are the recent developments within the cyber threat landscape?**

The cyber threat landscape has grown in size and sophistication over the last decades (Beggs, 2010). The number of attacks is still growing, due to the high dependency of organizations on their computer systems and developments such as the internet of things (Sophos, 2015; Verizon Enterprise, 2015). This growth has resulted into a lot of opportunities for cyber threat agents. These opportunities increase with the large amount of information on executing cyber risks, as well as the available software tools that could be used to perform a hack or another cyber risk.

A second important development in the cyber threat landscape is the growing influence of (inter)national regulations. These regulations compel organizations to increase the IT security of systems that process or store privacy related data.

5. **Which categorizations exist, and are applicable to categorize cyber threats?**

Several different cyber risk categorizations exist. These categorizations include individual threat categories (Information Security Forum, 2014; Muckin & Fitch, 2015), as well as categorizations based on the steps within a cyber risk (Lockheed Martin Corporation, 2015), or a more general division between the goal of a cyber risk (Clough, 2010). Within this research a combination between IRAM2 (Information Security Forum, 2014) and the cyber kill chain (Lockheed Martin Corporation, 2015) is used to categorize the threat events within a cyber risk scenario. The cyber kill chain provides information about the different stage of a threat event within the overall risk scenario and IRAM2 allowed us to categorize each individual threat event and therefore map it towards a potential control. The by Clough (2010) described cyber risk categories (unauthorized computer access, use of malicious software, disruption of service) is more high level and could therefore be applicable to categorize the entire cyber risk scenarios. A problem with this categorization is that it is not mutually exclusive and therefore difficult to apply. This problem is mainly caused since malicious software is often used as a tool to gain unauthorized computer access or to perform a denial of service attack. The general categorization of Clough (2010) is therefore not included in the taxonomy.

IRAM2 as well as some other threat categorizations include, as indicated above, predefined security measures to control these threats. This extra functionality could be useful during a risk analysis process. It is however important to investigate the individual threat events in the context of the entire risk scenario and the IT landscape of your organization in order to determine the needed security measure. The provided security measures per threat could however still provide valuable insights in possible ways to control the threat.

6. How can a cyber risk scenario be captured in a structured manner?

One of the important drivers of this research was to provide a structured format to capture cyber risk scenarios in a structured manner. This structure allows the reuse of (parts of) the earlier identified scenarios. We aimed to achieve this structured approach with the creation of a cyber risk taxonomy to capture a cyber risk scenario. The taxonomy, that was identified in the second sub research question, provides the concepts to capture cyber risk scenarios in a pre-defined, and structured, manner. The concepts are described in more detail by various variables, which are based on various sources. These different variables within the taxonomy are described in detail in Chapter 6.1.

Besides the provided structure a general approach is described to identify, describe, and capture a scenario within the taxonomy. The approach is based on the three general steps of a risk analysis approach (as identified in the first sub research question): identify, describe, and estimate. The identification step includes the, as Pfleeger et al. (2015) indicated, necessary combination between the threat-, asset-, and vulnerability based approach. These approaches are combined to allow an analyst to identify the organization's IT landscape (and vulnerabilities), the, for a threat agent interesting, assets, and at last the specific threat that could target their asset, given their IT landscape and cyber security measures. The structure of, and concepts in, the taxonomy will guide the analyst during this identification process. The identified risk scenarios and the threat events within the scenarios are further described during the description step. Once all the taxonomy elements are properly identified and described, the overall risk impact and probability can be estimated. The estimations are based on criminal theories (Cohen & Felson, 1979; Pfleeger et al., 2015) that indicate that a criminal act (like a cyber risk) only occurs if there is a motivation, opportunity, and a method. Variables to determine these three factors within a cyber risk scenario are captured in the taxonomy. A structured approach to use these elements to estimate an overall probability value is provided within a causal model that is addressed in the next (seventh) sub research question.

7. How can existing causal risk models be used to model cyber risk scenarios?

The cyber risk scenario within the taxonomy needed, as indicated in the conclusion of Chapter 6, a causal model to explicitly capture the relations between the different threat events. This sub research question identified the possibility to capture the defined cyber risk scenario within existing causal models. This study included a general quantitative- (Bayesian network), a risk based semi quantitative- (ANRAM), and a security risk specific, but qualitative (CORAS) model. The research confirmed that it is possible to use all these different models to capture and model a cyber risk scenario. The scenarios that resulted from these three models however varied a lot. It is therefore important to align the goal of the analysis together with the available resources to perform the analysis with the selection for one of those models. How each model could be used within a cyber risk analysis process is explained in Table 9.1.

The biggest difference between the three models is their level of complexity and detail, where the complexity is mainly caused by needed input to determine the probability and/or impact values. The construction of a Bayesian networks needed the most detailed input values to determine the probabilistic dependencies between the different elements in the scenario. Due to the scope of this research and the lack of structured cyber risk data to determine these values it was not possible to determine these detailed values. The probabilistic dependencies were therefore limited to qualitative dependencies and constraints within the Bayesian network. These qualitative dependencies provide a clear overview of the interplay of the contextual elements in a risk scenario with the overall scenario's probability. This contextual information was not explicitly captured in the ANRAM and the CORAS model. Both of these models were more focused towards the causal structure of, and the direct influence on, the threat events. A difference between these

models is the formal grounding of ANRAM versus the qualitative basis of the CORAS model. The risk assessment process within CORAS is performed via several brainstorm sessions that result into qualitative estimations (which are described within the CORAS method), but within ANRAM, this process is supported by the formal grounding and the propagation rules. These rules determine the overall plausibility and impact of the scenario. These values are determined by the loose arguments that are captured within the model.

Table 9.1: Main focus and application of the causal models

Model	Focus	Applications
Bayesian network	Estimate the probability values of and within a scenario	Create an overview to investigate the probability values in relation with the contextual factors
		Perform deeper analysis in to quantify the probability values of certain threat events
ANRAM	Determine the plausibility and impact of the overall scenario and individual arguments in the scenario	Further asses a potential risk model with evidence, (qualitative) claims, and other arguments to determine the plausibility as well as the potential impact
		Develop generalizations within a scenario, and reuse these generalizations in a new scenario
CORAS	Create an understandable overview of the risk and its consequences	Create an understandable risk scenario overview to communicate the risk events and its consequences with other stakeholders
		Create quick qualitative models to visualize the causal chain of threat events to identify the vulnerabilities within the scenario

The above described findings provide an answer for this sub research question. This research identified that it is possible to use both exact quantitative models, as well as qualitative models to capture a cyber risk scenario. It is therefore important to determine the needed level of detail of the output, as well as the available resources to determine such an output in order to select a more quantitative, or more qualitative based model.

9.2 Conclusion of the main research question

The sub research questions provided the research findings which are needed to answer the main research question within this thesis. The main research question was as follows:

What are the causal structures and the probabilities of typical cyber risk scenarios, and how can these be modeled and captured in a taxonomy?

This question covers three different components: the structure of cyber risk scenarios, the probability estimation of these scenarios, and the ability to capture and model these structured scenarios. The primary structure of the risk is the causal relation between the different threat events that cause a certain impact. This structure is based on, and applicable to, every generic risk (Fenton & Neil, 2013). Several approaches exist to categorize the individual threat events (e.g. IRAM2 (Information Security Forum, 2014)), as well as

the order of threat events within a cyber risk scenario (e.g. cyber kill chain (Lockheed Martin Corporation, 2015)). It was identified that the structure of threat events within a cyber risk scenario is very dynamic (due to the iterative way a threat agent works, and the large amount of possible threat events a threat agent can initiate) and, although the different steps of a cyber kill chain could be identified, the proposed order of the kill chain was not present within each cyber risk that was captured in the taxonomy during the data validation. This finding is in line with the described hacking approaches in 5.5.2. We can therefore conclude that the threat events within a cyber risk scenario can be related to the different steps in the cyber kill chain, but that it is not possible to map each cyber risk directly on the steps that are proposed by the cyber kill chain.

The second aspect of the research question addressed the probability values of and within a cyber risk scenario. During the study it was identified that the probability of a cyber risk scenario was not limited towards the different threat events in the scenario. This is due to the fact that a cyber risk can be seen as a criminal act, due to the fact that a cyber risk is a risk that is caused by a human with a malicious intent (Pfleeger et al., 2015). This indicates that the overall plausibility of a cyber risk scenario can be determined by the criminal theory of Cohen and Felson (1979). This theory indicates that the plausibility of such an attack is determined by the attacker's resources, the organization's vulnerabilities, and the motivation of initiating such an attack (the possible reward). The criminal theory of Cohen and Felson is related to cyber risk scenarios in multiple studies (Byres & Lowe, 2004; Choo, 2011; Pfleeger et al., 2015). During the remainder of the study we identified that this structure could be applied to determine a qualitative probabilistic dependency. This structure was explicitly captured by combining a set of taxonomy elements in the Bayesian network in Figure 7.4. Based on the proposed structure and the literature findings, it can be concluded that it is needed to include all three of the above mentioned factors (attacker, vulnerabilities, and reward/motivation) to estimate the probability of a cyber risk scenario.

The third part of the research question, capturing the stored cyber risk scenarios, was addressed during the development of the taxonomy in Chapter 6 and the application of the causal models in Chapter 7. This research identified that these scenarios can be captured in a taxonomy that consist of seven concepts, and 51 variables. The basic risk elements of the taxonomy were identified via the risk scenario concepts that resulted from the literature study, which is described in Chapter 4.2. These elements were further elaborated with the story elements of the study of De Kock (2014) to include the entire story of the risk. The cyber aspects were provided with the STIX framework (Barnum, 2014). The combination of these three factors resulted in a taxonomy that was able to capture the entire story of a cyber risk. The taxonomy's completeness was validated by capturing a set of 40 cyber incidents within the taxonomy, the incidents were gathered via Deloitte. A disadvantage of the taxonomy, which captured the entire story of the risk in a structured manner, is the lack of a clear overview of the causal structure of the threat events within the model. This causal structure, together with impact and probability estimations, can be captured within a causal model. The application of such a model to capture a cyber risk scenario is addressed in the research question as well. This research investigated the application of Bayesian networks, ANRAM, and the CORAS model to capture the causal structure of cyber risk scenarios. We were able, as indicated during the answer of the seventh sub research question, to tailor all three of these models to capture a cyber risk scenario to represent the causal structure and probability estimations of the threat events. A difference between these models was their focus and level of detail. A Bayesian network is able to calculate exact and detailed probability values, which represent the causal structure as well as the contextual structure of the risk scenario. A disadvantage of this level of detail is the detailed information that is needed to construct the model. A more qualitative oriented model like CORAS is able to provide a causal structure as well as probability and impact estimations. This model provides less details in their probability and impact

estimation, and therefore requires less detailed and complex approaches to estimate these values, which makes CORAS easier to apply in practice. The third model, ANRAM, can be defined as semi-quantitative model and provides a useful framework to assess an overall cyber risk scenario based on the different arguments within the scenario. Although ANRAM is easier to apply in practice the possibilities within this model are more limited, compared to the Bayesian network.

Based on the proposed models we can conclude that the use of such a model is dependent on both the goal of the analysis: provide exact probability estimations or create a quick and understandable overview of the cyber risk scenario. As well as the available resources to construct the model. Within our research the Bayesian network was the best model to capture both the causal structure of the threat events and the interplay between the attacker's capabilities, organization's vulnerabilities, and the possible reward of the cyber risk. We were able to determine the qualitative dependencies in the Bayesian network, a complete Bayesian network requires more detailed information, which our research could not provide. We therefore conclude that the proposed uses of ANRAM, as a risk assessment approach, or the CORAS model, to support a risk analysis approach, are better suited in practice, but that the Bayesian network model of a cyber risk scenario provides more possibilities for future research.

10. DISCUSSION

The creation of the cyber risk taxonomy and cyber scenario model in this research has provided several valuable insights. There are however some limitations to the conducted research. These limitations are addressed in this chapter. Besides these research limitations, an overview of future research possibilities is provided.

10.1 RESEARCH LIMITATIONS

As indicated above there are some limitations within this research. Some general limitations are concerned with the practical applicability of our research. The proposed taxonomy and scenario models are based on the performed literature review and although we performed validation interviews we did not perform a case study to confirm the usability of the proposed results. It was therefore not possible to formulate a conclusion about this matter. It was however according to our research approach and scope to identify the proposed taxonomy and models, without performing an experiment or case study to evaluate and validate their applicability. We did provide a literature review towards existing risk analysis methodologies, which allowed us to create the general descriptions in both Chapter 6 and 7 about applying the taxonomy and risk models. The fact that we did not perform an experiment is addressed in the future research section as well. The remainder of the research limitations are explained in terms of its validity. We have defined three groups of validity: Internal validity, External validity, and Reliability. The definitions for these three groups are based on the work of Yin (2003).

10.1.1 INTERNAL

The internal validity is concerned with the causal relationships between our research and its results. This indicates that the results from our study were not achieved by alternative explanations. The defined taxonomy as well as the application of this taxonomy in the causal models are the main results of our research. The biggest threat to the internal validity is caused by the fact that the concept's variables of the taxonomy as well as the causal models were not validated in detail during the validation interview. The reason that we did not validate the taxonomy's elements in detail during the interviews was time related. The goal of the validation interviews was to validate the business application of the overall taxonomy. It was not feasible to include each taxonomy concept and variable in this validation session. Another reason that this was omitted from the validation interviews was that the completeness of the taxonomy was addressed during the data validation, as explained in Chapter 8.2.

10.1.2 EXTERNAL

The external validity indicates if the research's findings are generalizable. The external validation interviews strengthened the external validity of our research. This was done by addressing the business application of the proposed taxonomy and scenario model to different experts from different organizations. The experts confirmed the need for such an approach and identified valuable applications of our findings. However, as indicated above there was no case study, or other experiment, conducted to assess the usability of the proposed taxonomy and scenario model.

One aspect that remains a threat to the external validity of our research is the construction of the variables for each concept within the taxonomy. The scales of the internal and external value were not based on earlier research, however most variables and concepts are based on other research or risk analysis methods. This was due to the fact that the literature and risk analysis methods that were identified in the literature review did not provide a scale that was applicable in the cyber risk context.

10.1.3 RELIABILITY

The reliability aspect within the research limitations refers to the repeatability and consistency of the performed research. It is important, for a scientific research, to identify the influence of the researchers on the proposed results. A threat towards the research's reliability that we encountered is related to the performed validation interviews. In this research it was decided to perform semi structured interviews to allow the possibility to tailor the interviews to the experiences and knowledge of the interviewee. A disadvantage of the limited structure in these interviews is that not every interviewee was asked the exact same questions. We were therefore not able to directly compare the interview's results. The choice for these semi structured interviews however did result into valuable insights about the experiences of the interviewees.

A second limitation that is related to the research reliability is concerned with the performed literature review. The performed literature was semi structured and conducted following the snowballing principle. This approach could have influenced the results of the literature review since the selection of the included literature was dependent on our opinions. This effect was limited by performing various unstructured interviews to analyze the founded literature. These interviews were performed within Deloitte with several experts on both the technical and business aspects of cyber security.

10.2 FUTURE RESEARCH

The performed research as described in this thesis developed into several future research opportunities. Within this research three future research opportunities are identified. First, the taxonomy's application can be captured in a structured method to construct these methods and use them in a risk analysis. Chapter 6, in which the taxonomy is described, includes a general description of the way in which the taxonomy could be used to create cyber risk scenarios, but this approach is limited and does not include an analysis aspect in which the created scenarios are actually used. Such a method should, besides the taxonomy, include one or more of the proposed scenario models to calculate the probability and impact values and to capture the causal structure of the risk scenario. Another advantage of such a method is the ability to validate the proposed taxonomy with one or more case studies. The case study, or another experiment that could be used to further evaluate and validate the different concepts of the taxonomy and structure of the scenario models, would provide valuable insights in the actual usability of the taxonomy and model.

The ability to use the structured data in the taxonomy to perform statistical analyses in the field of cyber probability and impact quantification can be seen as a second research opportunity. These analyses could result in insights that could be used during the estimation phase of a new risk analysis. It is however difficult to determine how fast an organization is able to create enough structured cyber risk scenarios of occurred incidents to develop a representing test group. An organization that performs the several cyber risk analyses, and investigations, for different organizations will gather this information faster. Another approach in which more structure data could be combined is via knowledge sharing between different organizations, as described in Chapter 3.1.4. During the validation interviews the added value of more knowledge sharing was confirmed. It was however indicated that this would most likely only succeed if an independent third party

organized this process (e.g. how the ISACs are organized by the NCSC (Nationaal Cyber Security Centrum, 2015)). The data structure of the taxonomy could be captured within a repository and used by the third party. However, further research into the practical knowledge sharing abilities of the proposed taxonomy and scenario models is required to construct conclusions about these abilities.

The third research opportunity lies in the field of cyber threat intelligence and automatically structuring unstructured cyber risk knowledge. In a recent news publication of IBM they have described how they are trying to apply Watson, a platform that can process natural language and uses machine learning to reveal insights from this natural language, to construct structured cyber knowledge out of a large amount of unstructured cyber risk sources (IBM, 2016). Watson was instructed to identify several components that are relevant within a cyber risk in the unstructured sources (e.g. blogs, textual reports, etc.). The concepts within the defined taxonomy could be used to identify and capture the relevant concepts of a cyber risk scenario.

REFERENCES

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

AgenaRisk. (2016). Agena: Bayesian network and simulation software for risk analysis and decision support. Retrieved from http://www.agenarisk.com/

Barnum, S. (2014). *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX ™)*.

Bau, J., & Mitchell, J. C. (2011). Security Modeling and Analysis. *Security & Privacy, IEEE*, *9*(3), 18–25.

Beggs, P. (2010). *Securing the Nation's Critical Cyber Infrastructure*.

Bell, D. (2004). *Cyberculture: The key concepts*. Psychology Press.

Bex, F. J. (2011). *Arguments, stories and criminal evidence: A formal hybrid theory* (Vol. 92). Springer Science & Business Media.

Bex, F. J., & Hovestad, B. (2016). An Argumentative-Narrative Risk Assessment Model. In *Proceedings of the European Intelligence and Security Informatics Conference (EISIC)*. IEEE Press, to appear.

Bex, F. J., Koppen, P. J. Van, Prakken, H., & Verheij, B. (2010). A hybrid formal theory of arguments, stories and criminal evidence. *Artificial Intelligence and Law*, *18*(2), 123–152. http://doi.org/10.1007/s10506-010-9092-x

Bex, F. J., & Renooij, S. (2016). From Arguments to Constraints on a Bayesian network. In *Proceedings of COMMA 2016, Frontiers in Artificial Intelligence and Applications*. To appear.

Braber, F. Den, Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps — a guided tour to the CORAS method. *BT Technology Journal*, *25*(1), 101–117.

Brockett, P. L., Golden, L. L., & Wolman, W. (2012). Enterprise Cyber Risk Management. In D. J. Emblemsvag (Ed.), *Risk Management for the Future - Theory and Cases* (pp. 319–340). InTech.

Byres, E., & Lowe, J. (2004). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In *Proceedings of the VDE Kongress* (pp. 213–218).

Cheung, S., Lindqvist, U., & Fong, M. W. (2003). Modeling Multistep Cyber Attacks for Scenario Recognition. In *Proceedings of the Third DARPA Information Survivability Conference and Exposition (DISCEX III)* (Vol. 1, pp. 284–292). Washington, D.C.: IEEE.

Choo, K. K. R. (2007). Zombies and botnets. *Trends and Issues in Crime and Criminal Justice*, (333).

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

Clough, J. (2010). *Principles of Cybercrime*. Cambridge University Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, *44*(4), 588–608.

COSO. (2012a). *Risk Assessment in Practice*.

COSO. (2012b). *Understanding and Communicating Risk Appetite*.

Dandurand, L., & Serrano, O. S. (2013). Towards Improved Cyber Security Information Sharing. In K. Podins, J. Stinssen, & M. Mayboum (Eds.), *5th International Conference on Cyber Conflict (CyCon)* (pp. 1–16). IEEE.

Davidson, M., & Schmidt, C. (2014). *TAXII Overview*.

De Kock, P. A. M. G. (2014). *Anticipating criminal behaviour: Using the narrative in crime-related data*. Tilburg center for Cognition and Communication (TiCC).

Druzdzel, M. J., & Van Der Gaag, L. C. (2000). Building Probabilistic Networks : "Where Do the Numbers Come From ?" *IEEE Transactions on Knowledge and Data Engineering*, *12*(4), 481–486.

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). A comparative framework for risk analysis methods. *Computers & Security*, *12*, 597–602.

ENISA. (2013). *Threat Landscape Overview of current and emerging cyber-threats*. http://doi.org/10.2788/14231

Fenton, N., & Neil, M. (2013). *Risk assessment and decision analysis with Bayesian networks*.

Fenton, N., Neil, M., & Lagnado, A. (2013). A General Structure for Legal Arguments About Evidence Using Bayesian Networks. *Cognitive Science*, *37*(1), 61–102. http://doi.org/10.1111/cogs.12004

Franqueira, V. N. L., Tun, T. T., Yu, Y., Wieringa, R., & Nuseibeh, B. (2011). Risk and Argument : A Risk-based Argumentation Method for Practical Security. *Requirements Engineering Conference (RE), 19th IEEE*, 239–248.

Haley, C. B., Laney, R., & Moffett, J. D. (2008). Security Requirements Engineering : A Framework for Representation and Analysis. *IEEE Transactions on Software Engineering*, *34*(1), 133–153. http://doi.org/10.1109/TSE.2007.70754

Hevner, A. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*, *19*(2), 87–92.

Hovestad, B., & Bex, F. J. (2016). *Making sense of risk: A hybrid argumentative-narrative approach to risk assessment. Utrecht University Technical report UU-CS-2016-006*.

Howard, R. A., & Matheson, J. E. (2005). Influence Diagrams. *Decision Analysis*, *2*(3), 127–143. http://doi.org/10.1287/deca.1050.0020

IBM. (2016). IBM Watson to Tackle Cybercrime. Retrieved July 2, 2016, from https://www.ibm.com/news/ca/en/2016/05/10/a700944w74684b00.html

Information Security Forum. (2014). *IRAM2: The next generation of assessing information risk*.

Information Security Forum. (2015). *Threat Horizon 2018*.

IRM. (2002). *A Risk Management Standard*.

ISACA. (2015). Glossary. Retrieved January 26, 2016, from http://www.isaca.org/Pages/Glossary.aspx?char=A

ISO /IEC 27001. (2013). *International Standard: Information technology — Security techniques — Information security management systems — Requirements*.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147–159. http://doi.org/10.1016/j.cose.2004.07.004

Kjaerfulff, U. B., & Madsen, A. L. (2005). *Probabilistic Networks — An Introduction to Bayesian Networks and*

Influence Diagrams. Aalborg University.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471–476. http://doi.org/10.1007/s10669-013-9485-y

Lockheed Martin Corporation. (2015). *Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform*.

Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-Driven Risk Analysis*. Springer.

McAfee. (2014). *Net Losses : Estimating the Global Cost of Cybercrime*.

Mcqueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A. (2005). Time-To-Compromise Model For Cyber Risk Reduction Estimation. In *Quality of protection* (pp. 49–64). Springer US.

Microsoft. (2005). The STRIDE Threat Model. Retrieved April 7, 2016, from https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

Moore, R. (2010). *Cybercrime Investigating high-technology computer crime*. Routledge.

Muckin, M., & Fitch, S. C. (2015). *A Threat-Driven Approach to Cyber Security*.

Nationaal Cyber Security Centrum. (2015). ISAC's - Information Sharing and Analysis Centres. Retrieved May 20, 2016, from https://www.ncsc.nl/samenwerking/publiek-private-samenwerking/isacs.html

Neil, M., Fenton, N., & Nielson, L. (2000). Building large-scale Bayesian networks. *The Knowledge Engineering Review*, *15*(1999), 257–284.

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

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

Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. *Organization Sciences*, *5*(1), 14–37.

OWASP. (2015a). OWASP Risk Rating Methodology. Retrieved January 18, 2016, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

OWASP. (2015b). Threat Risk Modeling. Retrieved January 12, 2016, from https://www.owasp.org/index.php/Threat_Risk_Modeling

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing*. Prentice Hall.

Ponemon Institute. (2015). Cost of Cyber Crime Study: Global. *Hewlett Packard Enterprise*, (October).

PWC. (2015). *Cyber Security: Building confidence in your digital future*.

Rausand, M. (2011). *Risk assessment - Theory, Methods, and Applications*. John Wiley & Sons.

Roxburgh, C. (2009). The use and abuse of scenarios. *McKinsey Quarterly*, *November*, 1–10.

SANS Institute. (2007). *Web Based Attacks*.

SANS Institute. (2015). *CIS Critical Security Controls 6.0*.

Shachter, R. D. (1986). Evaluating Influence Diagrams. *Operations Research*, *34*(6), 871–882.

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

Sophos. (2015). *Security Threat Trends 2015*.

Suh, B., & Han, I. (2003). The IS risk analysis based on a business model. *Information & Management*, *41*,

149–158.

The MITRE Corporation. (2015). Common Attack Pattern Enumaration and Classification. Retrieved May 17, 2016, from https://capec.mitre.org/

Verheij, B., Bex, F. J., Timmer, S. T., Vlek, C. S., Meyer, J. C., Renooij, S., & Prakken, H. (2016). Arguments , scenarios and probabilities : connections between three normative frameworks for evidential reasoning. *Law, Probability, and Risk*, *15*(1), 35–70.

Verizon Enterprise. (2015). *Data Breach Investigation Report*.

Verizon Enterprise. (2016). Veris - The Vocabulary for Event Recording and Incident Sharing. Retrieved March 21, 2016, from http://veriscommunity.net/index.html

Verschuren, P., & Doorewaard, H. (2010). *Designing a Research Project* (Second edi). The Hague: Eleven International Publishing.

Vlek, C., Prakken, H., Renooij, S., & Verheij, B. (2013). Modeling Crime Scenarios in a Bayesian Network. In *Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law* (pp. 150–159). Rome, Italy: ACM.

Vlek, C., Prakken, H., Renooij, S., & Verheij, B. (2015). Constructing and Understanding Bayesian Networks for Legal Evidence with Scenario Schemes. In *Proceedings of the 15th International Conference on Artificial Intelligence and Law* (pp. 128–137). ACM.

Wohlin, C. (2014). Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering* (pp. 38–48). ACM.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (3th editio). SAGE Publications, Inc.

APPENDIX

A. OVERVIEW OF CYBER RISK CATEGORIES

Described threats and controls within IRAM2 (Information Security Forum, 2014)

Threat event type	Threat event	Sophistication	Controls
Authentication attacks	Session hijacking	Moderate	CTL11 Encryption (communications) CTL22 Management of secure software development CTL18 Security testing CTL01 Secure network design CTL06 Wireless network security CTL05 Secure standardized system builds CTL03 Event logging and monitoring CTL04 IDS/IPS CTL07 Security awareness
	Unauthorized access to legitimate authentication credentials	High	CTL23 Access management CTL18 Security testing CTL05 Secure standardized system builds CTL20 Encryption (storage) CTL01 Secure network design CTL06 Wireless network security CTL03 Event logging and monitoring CTL04 IDS/IPS CTL07 Security awareness
	Exploit vulnerable authorization mechanisms	Moderate	CTL22 Management of secure software development CTL23 Access management CTL03 Event logging and monitoring CTL04 IDS/IPS CTL18 Security testing CTL20 Encryption (storage) CTL01 Secure network design CTL05 Secure standardized system builds CTL06 Wireless network security CTL07 Security awareness
Communications attacks	Unauthorized monitoring and/or modification of communications	High	CTL11 Encryption (communications) CTL03 Event logging and monitoring CTL01 Secure network design CTL06 Wireless network security CTL18 Security testing CTL04 IDS/IPS CTL05 Secure standardized system builds CTL10 Physical security CTL07 Security awareness CTL22 Management of secure software development

Threat event type	Threat event	Sophistication	Controls
Denial of Service	Conduct a denial of service (DoS) attack	Moderate	CTL01 Secure network design CTL12 Availability and capacity management CTL03 Event logging and monitoring CTL04 IDS/IPS CTL05 Secure standardized system builds CTL13 Business continuity/disaster recovery CTL09 Incident management
Information leakage	Exploit insecure disposal of an organization's information assets	Moderate	CTL02 Information asset management CTL07 Security awareness CTL20 Encryption (storage) CTL22 Management of secure software development
Malware	Introduce malware to information systems	Low	CTL08 Malware protection CTL05 Secure standardized system builds CTL14 Vulnerability management CTL03 Event logging and monitoring CTL04 IDS/IPS CTL18 Security testing CTL07 Security awareness CTL15 Mobile device security CTL01 Secure network design CTL09 Incident management CTL22 Management of secure software development CTL13 Business continuity/disaster recovery CTL16 Backup management
Misconfiguration	Exploit misconfigured organizational information systems	Moderate	CTL05 Secure standardized system builds CTL14 Vulnerability management CTL19 Change management CTL18 Security testing CTL03 Event logging and monitoring CTL04 IDS/IPS CTL01 Secure network design CTL09 Incident management CTL16 Backup management CTL13 Business continuity/disaster recovery
	Exploit design or configuration issues in an organization's remote access service (e.g. VPNs)	High	CTL01 Secure network design CTL05 Secure standardized system builds CTL19 Change management CTL14 Vulnerability management CTL18 Security testing CTL03 Event logging and monitoring CTL04 IDS/IPS CTL09 Incident management
	Exploit poorly-designed network architecture	Moderate	CTL01 Secure network design CTL05 Secure standardized system builds CTL02 Information asset management CTL03 Event logging and monitoring CTL04 IDS/IPS CTL18 Security testing

Threat event type	Threat event	Sophistication	Controls
Misuse	Misuse of information systems	Low	CTL23 Access management CTL03 Event logging and monitoring CTL16 Backup management CTL05 Secure standardized system builds CTL20 Encryption (storage) CTL02 Information asset management CTL18 Security testing CTL24 Employment screening CTL01 Secure network design
Physical	Unauthorized physical access to information systems	Moderate	CTL10 Physical security CTL07 Security awareness CTL03 Event logging and monitoring CTL20 Encryption (storage) CTL05 Secure standardized system builds
	Physical damage to or tampering with information systems	Low	CTL10 Physical security CTL13 Business continuity/disaster recovery CTL09 Incident management CTL16 Backup management CTL03 Event logging and monitoring CTL05 Secure standardized system builds
	Theft of information system hardware	Low	CTL10 Physical security CTL05 Secure standardized system builds CTL13 Business continuity/disaster recovery CTL16 Backup management CTL20 Encryption (storage) CTL03 Event logging and monitoring
	Conduct physical attacks on organizational facilities or their supporting infrastructure	Moderate	CTL10 Physical security CTL13 Business continuity/disaster recovery CTL16 Backup management CTL21 Environmental security
Reconnaissance / information gathering	Unauthorized network scanning and/or probing	Negligible	CTL05 Secure standardized system builds CTL03 Event logging and monitoring CTL04 IDS/IPS CTL01 Secure network design CTL02 Information asset management
	Gathering of publically-available information about an organization	Negligible	CTL07 Security awareness CTL02 Information asset management
Social engineering	Phishing	Low	CTL07 Security awareness CTL08 Malware protection CTL01 Secure network design CTL23 Access management
	Insert subversive individuals into organizations	Moderate	CTL24 Employment screening CTL23 Access management CTL07 Security awareness CTL03 Event logging and monitoring CTL02 Information asset management CTL20 Encryption (storage)
	Interpersonal manipulations	Low	CTL07 Security awareness

Threat event type	Threat event	Sophistication	Controls
Software exploitation	Exploit vulnerabilities in an organization's information systems	Low	CTL22 Management of secure software development CTL14 Vulnerability management CTL05 Secure standardized system builds CTL18 Security Testing CTL07 Security awareness CTL01 Secure network design CTL03 Event logging and monitoring CTL04 IDS/IPS CTL08 Malware protection CTL15 Mobile device security CTL13 Business continuity/disaster recovery CTL16 Backup management CTL09 Incident management
Supplier compromise	Compromise supplier or business partner of target organization	High	CTL17 External supplier security CTL22 Management of secure software development

B. TAXONOMY SCALES AND CATEGORIES

Concept	Variable	Scale/category options
General scenario	Timeline	Minutes – Hours – Days – Weeks – Months
General scenario	Scenario type	Incident – Risk analysis
Organizational information	Size - Employees	(0 - 100) – (101 – 500) – (500 – 1500) – (1500 - +)
Threat agent	Type	Cyber-criminal – Script kiddie – Nation State – Corporation – Hacktivist – Grey hat hacker
Threat agent	Motivation	Making a statement – Gain competitive advantage – Espionage – Disruption – Financial gain
Threat agent	Skills	Security penetration skills (9) – network and programming skills (7) – advanced computer user (5) – some technical skills (3) – no technical skills (1)
Threat agent	Resources	Normal computer user (3) – funded group of hackers (6) – State sponsored attack (9)
Asset	Category	Financial data – Intellectual property – Sensitive operational information – Services – Brand image – Personally identifiable information
Asset	Accessibility	External – Internal – Privileged
Asset	Encryption	Yes – No – Unknown
Asset	Internal value	Negligible – Low – Medium - High
Asset	External value	Negligible – Low – Medium - High
Threat event	Stage	Reconnaissance – Preparation – Delivery – Exploitation – Installation – Act on objective
Threat event	Type	Authentication attacks – Communications attacks – Denial of Service – Information leakage – Malware – Misconfiguration – Misuse – Physical – Reconnaissance / information gathering – Social engineering – Software exploitation – Supplier compromise
Threat event	Technical impact	Confidentiality – Loss of system security – Integrity - Availability
Threat event	Sophistication	Negligible – Low – Medium - High
Threat event	Modus	Social – Malware – Hacking – Physical
Business impact	Financial	Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
Business impact	Non compliance	How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
Business impact	Reputational	Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
Vulnerability	Type	Social – Technical
Vulnerability	Ease of exploit	Theoretical (1), difficult (3), easy (5), automated tools available (9)

Vulnerability	Awareness	Unknown (1), hidden (4), obvious (6), public knowledge (9)
Control	Type	Detective – Preventive – Reactive

C. BAYESIAN NETWORK NPTS

Method NPT

Skills:		**1**				**2**				**3**				**4**			
Resources:		**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Method	**True**																
	False																

Opportunity NPT

Vulnerability:		**1**				**2**				**3**				**4**			
Control:		**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Opportunity	**True**																
	False																

Motivation NPT

Asset value:		**1**		**2**		**3**		**4**	
Other motivation:		**True**	**False**	**True**	**False**	**True**	**False**	**True**	**False**
Motivation	**True**								
	False								

D. CORAS MODELING LANGUAGE

Icons within the CORAS modeling language

Qualitative and quantitative likelihood estimations within CORAS

Likelihood value	Description	Definition
Certain	Five times or more per year	[50, ∞> : 10*y* = [5,∞> : 1*y*
Likely	Two to five times per year	[20, 50> : 10*y* = [2, 5> : 1*y*
Possible	Less than twice per year	[5, 20> : 10*y* = [0.5, 2> : 1*y*
Unlikely	Less than once per two years	[1, 5>: 10*y* = [0.1, 0.5> : 1*y*
Rare	Less than once per ten years	[0, 1> : 10*y* = [0, 0.1> : 1*y*

Impact values and example estimation descriptions of health records within CORAS

Impact value	Description
Catastrophic	1000+ health records are affected
Major	101–1000 health records are affected
Moderate	11–100 health records are affected
Minor	1–10 health records are affected
Insignificant	No health records are affected

E. ANRAM: PROPAGATION RULES AND PLAUSIBILITY AND IMPACT SCALES

Propagation rules within ANRAM (Hovestad & Bex, 2016)

Rule	Description	Example
1	A piece of evidence E propagates P to a direct conclusion C.	E (P=0.8) that supports C, instantiates C as C (P=0.8).
2	A risk factor/claim X propagates P to a direct conclusion C.	X (P=1.0) that supports C, instantiates C as C (P=1.0).
3	If more than one premise (i.e. risk factor/claim, evidence) supports a conclusion C, then the premise with the highest P value is selected.	If we have some evidence E (P=0.8) and a risk factor X (P=1.0), we select X so we obtain C (P=1.0).
4	When using links through an AND function, the premise with the lowest P value is selected.	If we have a risk factor X (P=0.8) and a risk factor Y (P=1.0), we select X so we obtain C (P=0.8).
5	When using links through an OR/XOR function, the premise with the highest P value is selected.	If we have a risk factor X (P=0.8) and a risk factor Y (P=1.0), we select Y so we obtain C (P=1.0).
6	A premise X defeats a premise Y if and only if PX > PY.	A claim X(P=1.0) that attacks a risk factor Y(P=0.8) defeats Y.
7	The I value is determined by selecting the highest I value of the arguments that are not defeated.	If we have arguments X (I=0.6), Y (I=1.0), and Z (I=0.8), we obtain C (I=1.0).

Plausibility scales within ANRAM (Hovestad & Bex, 2016)

P Value	Indication
0.2	No substantial evidence available, the plausibility of the event occurring is small.
0.4	No substantial evidence available, the plausibility of the event occurring is medium.
0.6	Different claims and information from reliable evidence sources, the plausibility of the event occurring is medium.
0.8	Substantial evidence to support and confirm that the event might occur. The time and place are unknown. The plausibility of the event occurring is high.
1.0	Very strong evidence to support and confirm that the event might occur. The time and place are known. The plausibility of the event occurring is very high.

Impact scales within ANRAM (Hovestad & Bex, 2016)

I Value	Indication
0.2	Negligible
0.4	Minor
0.6	Moderate
0.8	Significant
1.0	Severe

F. VALIDATION PROTOCOL

The interviews will be semi-structured. This indicates that the questions below will form the guideline through the interview, but will not limit the interview.

Goal of the validation

Identifying the practical applicability of the created cyber risk scenarios

Agenda

- Introduction 5 min
- Introduction of my research
- Validation questions:
    - Current situation at the client side
    - Cyber risks scenarios (and my taxonomy)
        - How could risk scenarios be applied?
        - Discussing the structure of my taxonomy
    - Cyber risk scenario knowledge sharing
        - Advantages and disadvantages of knowledge sharing
        - Current situation regarding knowledge sharing

Questions

Current situation at the organization

1. How are cyber related risk analyses performed within COMPANY?
    - Which methods and approaches are used to perform these analyses?
        - Advantages and disadvantages?
    - Which problems are countered during the identification of relevant cyber risks?
    - How would an ideal risk analysis for COMPANY be performed?

Cyber risk scenarios

2. Could scenario based risk analyses be applied within COMPANY?
    - Are such cyber scenarios complete enough to provide an overview of the risks, targets, and vulnerabilities?
    - Which information within a scenario is crucial to underpin security related decisions?

3. Do you think it is possible to construct relevant as well as plausible cyber risk scenarios within the current security team?
    - Given the technical (hacking) knowledge?
    - Given the knowledge of the current IT landscape?
    - Which purpose could be achieved with the identified cyber risk scenarios?

4. Which elements are most crucial within a cyber risk scenario?

Cyber risk related knowledge sharing

5. What would be a motivation to share cyber related knowledge with other companies?
    - What could be disadvantages/dangers when such knowledge is shared?

- What factors would determine that you would (not) share such knowledge?

6. Which elements within shared cyber risk scenarios would make the knowledge more valuable?
   - Which elements would determine the relevance of this knowledge?
   - In what form would you like to review these scenarios? (plain text, qualitative/quantitative model)

G. VALIDATION INTERVIEW SUMMARIES

Note, with one exception are the provided summaries in Dutch. The information from these interviews is synthesized and described in Chapter 8.1.2.

INTERVIEW 1

HUIDIGE SITUATIE OP HET GEBIED VAN CYBER RISICO ANALYSES

Het cybersecurityteam bestaat uit een twee componenten. Een incident response team, en een cyber crime taskforce. Het tweede team verzorgt de proactieve risicoanalyses. Zo'n analyse start met het identificeren van de potentiële aanvallers (waarbij de focus ligt op hun motivatie en capabilities). Daarna wordt er gekeken naar de crown jewels van een bedrijf. Hierbij is het belangrijk om te beseffen dat er een verschil in waarde voor het bedrijf, en voor de aanvaller kan zijn. Zodra er een beeld is van deze twee componenten wordt er gekeken naar de dreigingen in het threat landschap door middel van threat intelligence. Dit houdt in dat er zoveel mogelijk relevante informatie wordt gezocht op het gebied van cyber dreigingen.

Voor het in kaart brengen van de dreigingen zijn verschillende aanpakken. Zo wordt er aan de hand van de cyber kill chain (Lockheed Martin) gekeken uit welke stappen een aanval bestaat, maar worden ook best practices gebruikt (zoals de SANS top 20, of ISO standaarden). Op basis van deze gecombineerde informatie worden de dreigingen in kaart gebracht in een kwadrant die aangeeft hoe urgent de dreiging is, en hoe 'goed' de controls momenteel zijn.

Dat overzicht kan worden verwerkt in een plan van aanpak.

HOE KUNNEN RISICO SCENARIO'S IN DE PRAKTIJK GEBRUIKT WORDEN?

Zaken die je moet weten om een risico scenario te gebruiken voor een advies:

- De verschillende stappen die een aanvaller heeft ondernomen om tot zijn doel te komen
- Hoe en wat voor communicatie er naar buiten is gegaan
- Wat het doel was van de aanval
- Type aanvaller
- Hoe is de informatie is weggesluisd vanuit de organisatie of andere acties zijn uitgevoerd.
- Overige specifieke technische malware details (IP's, Signatures, locaties, communicatie etc)

WAT IS DE TOEGEVOEGDE WAARDE VAN DERGELIJKE RISICO SCENARIO'S?

Er wordt momenteel al steeds meer gebruik gemaakt van scenario's. Hiervoor wordt onder andere de cyber kill chain gebruikt. Ook wordt er gekeken naar incidenten die zich bij andere organisaties hebben voorgedaan. Er wordt dan gekeken of dat incident hier ook had kunnen gebeuren.

Scenario's zijn vooral nuttig om de systemen extra te beschermen. Standaard (niet geavanceerde) aanvallen kan je namelijk via een goede standaard bescherming (virusscanner, gepatchte systemen, etc.) wel afstoppen. Echter zullen de geavanceerdere aanvallen hierdoor niet gestopt worden. Door dergelijke scenario's op te stellen en indien nodig hierop te reageren, kan dit wel.

Momenteel wordt er wel al gewerkt met Top Risico's. Hier wordt wel al heel positief op gereageerd vanuit sr Management. De 'top risico's geven een goed overzicht van de relevante dreigingen en hun mogelijke impact.

Top Risico's worden gevoed, gevalideerd en ingeschat op basis van aanvalsscenario's Er is echter nog geen vaste structuur die gebruikt wordt om deze scenario's weer te geven. Een scenario kan de patronen van een

aanval in kaart brengen. Wanneer dergelijke patronen bekend zijn, kunnen aanvallen ook sneller worden herkend bij een organisatie.

HOE KAN HET DELEN VAN CYBER RISICO INFORMATIE BIJDRAGE CYBER RISICO MANAGEMENT?

Kennis op het gebied van cyber wordt al gedeeld via ISAC's en overige partners. Dit gebeurt grotendeels wel ongestructureerd. De gestructureerde informatie die wordt gedeeld is gebeurd vaak via een derde partij (bijv. algemene lijsten met blacklists). Hele scenario beschrijvingen van incidenten worden nu nog niet geautomatiseerd gedeeld. Een reden hiervoor is dat de scenario's te divers zijn, om in een format te stoppen en te analyseren (en de aantallen dit nog niet noodzakelijk maken). Het zal dus nog steeds menswerk kosten om dergelijke scenario's op te stellen en te analyseren.

Het is echter wel waardevol om dergelijke risico scenario's te delen. Aan de hand van dergelijke scenario's kan namelijk worden gekeken of een dergelijk incident bij het eigen bedrijf zich voor kan doen (of misschien al doet). En is weer input om, indien nodig, de maatregelen bij te stellen.

INTERVIEW 2

HUIDIGE SITUATIE OP HET GEBIED VAN CYBER RISICO ANALYSES

Op dit moment worden risicoanalyses op een meer klassieke manier uitgevoerd. Dit houdt in dat er gekeken wordt naar bekende dreigingen en kwetsbaarheden. Op basis hiervan worden de beveiligingseisen van applicaties en dergelijke opgesteld. Er wordt hier echter breder gekeken dan alleen cyber. Elementen zoals aardbevingen, stroomstoringen, maar ook fouten van mensen worden meegenomen in het proces.

Het algemene beeld is in gebaseerd op het dreigingsbeeld van de NCSC.

Het doel van de huidige risicoanalyses is het beschermen van de beschikbaarheid van de applicaties en de vertrouwelijkheid van informatie.

HOE KUNNEN RISICO SCENARIO'S IN DE PRAKTIJK GEBRUIKT WORDEN?

Hiervoor is een goed beeld van het IT-landschap nodig. Deze kennis is nu vooral impliciet aanwezig. Er zijn wel delen in kaart gebracht, maar niet het totale geheel. Het grote probleem met een dergelijk overzicht is dat het erg goed moet worden bijgehouden (de kern zal niet snel veranderen, maar de losse applicaties veranderen wel vaak). Hierdoor wordt er vaker gewerkt met losse overzichten met meer detail.

Impliciet worden er nu wel risico scenario's gebruikt. Deze scenario's zijn niet expliciet uitgewerkt. Wel is er goed gekeken wat er eerder gebeurd is, en op basis van deze scenario's zijn er standaard werkinstructies opgesteld. Dit houdt in dat als er een threat zich voordoet (zoals een phishing mail) dat er al vast staat welke acties moeten volgen.

De risico scenario's zouden wel goed gebruikt kunnen worden in het bewust maken van de gevolgen van cyber risico's. Door dergelijke scenario's te gebruiken kan iemand laten zien welke gevolgen een cyber risico kan hebben, en waardoor bepaalde maatregelen dus nodig zijn. Voor een gebruiker zal dit meer begrip geven voor de benodigde extra behandelingen, en voor de directie geeft dit reden om hier budget voor te reserveren.

Echter is het grootste deel van de cyberaanvallen al redelijk bekend. Er komen weinig 'niet-voorziene' incidenten voor. Het zoeken naar nieuwe scenario's zal daarom niet direct veel extra problemen oplossen. Aan de andere kant is het met dergelijke scenario's wel mogelijk om proactief naar problemen te kijken. Nu wordt er namelijk meer gekeken naar wat er al gebeurd is, of welke bekende dreigingen er zijn, maar bij dergelijke risico's kan er ook gekeken worden naar wat er in de toekomst kan gebeuren.

WAT IS DE TOEGEVOEGDE WAARDE VAN DERGELIJKE RISICO SCENARIO'S?

- Expliciete kennis is beter bruikbaar voor meerdere doeleinde (communicatie, analyse van zwakheden, opstellen van business case).
- Scenario kan vertaald worden naar een werkinstructie, als je weet dat een begin stap van een scenario zich voordoet, kan je beter inschatten wat je nog kan verwachten.
- Hierbij is het erg belangrijk om duidelijk te maken wat de symptomen van zo'n scenario waren. Aan de hand van deze symptomen kan worden bepaald wanneer een dergelijk scenario zich weer voordoet.
- Op dit moment wordt er erg veel vallende wijs geleerd. Dit houdt in dat er gekeken wordt tegen welke problemen je aan bent gelopen, en dat je die in de toekomst gaat proberen te voorkomen. Dit wil je echter voor zijn, het delen van kennis kan hierbij helpen.

HOE KAN HET DELEN VAN CYBER RISICO INFORMATIE BIJDRAGE CYBER RISICO MANAGEMENT?

Kennis deling is erg waardevol om dergelijke scenario's proactief te gebruiken. Er kan dan namelijk worden geleerd van een grote groep organisaties, in plaats van alleen de eigen organisatie. Hierdoor kan je veel problemen dus ook al voor zijn. Zo kunnen Nederlandse bedrijven zich bijvoorbeeld al voorbereiden op risico scenario's die in andere landen al vaak voor komen maar in Nederland 'nog' niet.

Momenteel wordt kennis wel gedeeld via ISAC's. Dit gebeurt echter beperkt en erg impliciet. Er zou meer kennis op dit gebied moeten worden gedeeld. Een reden dat dit niet gebeurt, kan komen doordat ze bang zijn dat de informatie verkeerd wordt gebruikt. De gedeelde risico's geven immers zwakheden binnen een bepaalde organisatie aan.

INTERVIEW 3

HUIDIGE SITUATIE OP HET GEBIED VAN CYBER RISICO ANALYSES

Momenteel is cyber security nog niet heel erg risico gedreven. Er wordt meer gekeken naar het opbouwen van een basisverzekering, en het zorgen voor gepatchte systemen en een monitoringsysteem dat naar behoren werkt. Daarnaast zitten ze nu midden in een traject om een centraal managed securityprovider te integreren. Er is een externe partij geselecteerd die dit gaat oppakken.

Er is wel ooit gebruik gemaakt van het Deloitte Cyber Resilience Framework. Hiermee wordt de link gelegd tussen de applicaties en welke beveiliging hierbij nodig is. Waarbij ene focus op return on investment is, het is dus vooral belangrijk wat de mogelijke impact van een potentieel risico is. Er is echter niet een jaarlijkse grote risicoanalyse wat het plan voor het jaar bepaald. Reden hiervoor is dat er veel veranderd is op IT-gebied binnen de organisatie, hierdoor heeft een standaard risicoanalyse nog niet heel veel zin.

HOE KUNNEN RISICO SCENARIO'S IN DE PRAKTIJK GEBRUIKT WORDEN?

Scenario's kunnen worden gebruikt om verder dan de basis beveiliging te kijken. Deze beveiliging houdt, zoals hierboven aangegeven vooral het patchen van systemen en zorgen voor een goede standaard beveiliging in.

De scenario's zijn wel erg waardevol als een cyber risico als aanval wordt gezien. Dit houdt in dat een aanvaller bepaalde capabilities, motivatie, en mogelijkheden heeft. Op basis daarvan kan een beeld worden gecreëerd van de zijn mogelijkheden. Echter is het wel heel lastig om te bepalen welke daders er zijn, en wat hun capabilities kunnen zijn.

De scenario's moeten bepaalde indicators of compromise aangeven, die je vervolgens in een systeem kan inladen. Een monitor systeem kan dergelijke incidenten dan in een vroeg stadium herkennen.

WAT IS DE TOEGEVOEGDE WAARDE VAN DERGELIJKE SCENARIO'S?

De toegevoegde waarde van cyber risico scenario's ligt in de mogelijkheid om ou-of-the-box te denken. Wanneer een dader namelijk een bepaald doel heeft, en dit graag genoeg wilt bereiken, zal hij ook creatief denken naar de mogelijkheden om dit te bereiken. Standaardlijsten zullen daarom niet alle mogelijkheden afdekken. Het is echter wel erg lastig om precies te bepalen wat het motief van een dader is. Dit motief kan namelijk erg variëren per organisatie of zelfs deel binnen een organisatie.

Daarnaast kan het waardevol zijn om met meerdere inzichten scenario's op te stellen. Mensen met dezelfde achtergrond kijken vaak naar dezelfde aspecten, iemand met een andere achtergrond kan daarom iets toevoegen.

Daarnaast moeten ze heel specifiek voor een bedrijf worden gemaakt. Anders zijn ze erg algemeen en niet zo waardevol. Hierbij is het belangrijk om een goed beeld te hebben van het IT-landschap van een bedrijf. Dit overzicht is echter lastig te bepalen. Ondanks dat er vaak diagrammen en architecturen zijn van de applicaties en systemen in dit landschap, is het vaak de situatie dat dit niet overeenkomt met de huidige situatie. Dit kan door veranderingen en/of fouten komen.

HOE KAN HET DELEN VAN CYBER RISICO INFORMATIE BIJDRAGE CYBER RISICO MANAGEMENT?

Het komt vaak voor dat vertrouwelijke informatie liever niet gedeeld wordt. Deze informatie geeft immers ook weer welke zwakheden er binnen een organisatie zijn. Binnen de ISAC's wordt dergelijke vertrouwensgevoelige informatie ingedeeld in verschillende categorieën: groen voor vrij delen, oranje voor vertrouwelijk, en rood voor alleen intern. Op die manier kan worden bepaald wat er wel en niet gedeeld kan worden.

Een ander belangrijk aspect is het creëren van een gelijke taal voor de communicatie. Je ziet nu bijvoorbeeld steeds vaker de termen TTP (tactic, tecnhique, procedure) terugkomen binnen cyber om een bepaald incident te beschrijven. Deze categorie komt vanuit defensie en geven een aantal indicators of compromise aan. Op basis van die standaard elementen kan er snel worden bepaald of de beschrijving relevant is.

INTERVIEW 4

HUIDIGE SITUATIE OP HET GEBIED VAN CYBER RISICO ANALYSES

Binnen **Bedrijf** is sinds een jaar een switch gemaakt in werkwijze op het gebied van cyber risicoanalyse. Eerst werd er gekeken naar bepaalde plekken waar waardevolle informatie staat, hier werd dan een C I A (Confidentiality, Integrity and Availability) analyse op los gelaten, echter bleek dit niet voldoende. Om die reden wordt er nu naar 'waardeketens' gekeken. Hiermee wordt gedoeld dat informatie zich niet op één plek bevindt, maar verspreidt tussen verschillende systemen/plekken. Een risicoanalyse moet zich dus niet beperken, maar kijken naar een heel proces (e.g. er kunnen nu precies genoeg admin accounts zijn, maar is dit ook nog zo over een of twee maanden?).

De risico's en zwakheden binnen deze keten worden in kaart gebracht en beschermd waar mogelijk. Een cruciaal punt is het testen van deze beveiliging via pen-testing en red teaming. Dit wordt via externe partijen gedaan om extra informatie binnen het bedrijf te halen. Er is echter wel al een start met een intern pen test team. Hier wordt zowel vanuit de techniek gemeten (bijv. pen testing) als vanuit het proces (vaker meten en vergelijken of de situatie niet ongewild veranderd).

HOE KUNNEN RISICO SCENARIO'S IN DE PRAKTIJK GEBRUIKT WORDEN?

De nieuwe analysemethode lijkt meer in lijn met mijn scenario's. Er wordt immers niet meer gekeken naar losse elementen, maar naar een bepaalde situatie (de flow van informatie, en hoe deze toegankelijk is).

Een mooie extra toevoeging hieraan is het gebruiken van monitoring. Met monitoring worden bepaalde technische aspecten continu in de gaten gehouden voor raar gedrag. Wanneer nodig wordt er een maatregel genomen. Er zijn al use cases (scenario's) beschikbaar voor dergelijke monitoringsystemen. Deze use cases combineren de input van verschillende gemonitorde systemen om beter te reageren op potentiele incidenten). Echter beperken cyber risico's zich niet tot technische aspecten die te monitoren zijn. Wanneer er scenario's automatisch verwerkt kunnen worden die een combinatie kunnen maken tussen technische aspecten en business aspecten kan het monitoringsysteem verreikt worden. Een voorbeeld hierbij is het reageren op een phishing mail. Wanneer er een phishing mail is verstuurd is de kans op specifieke vervolg aanvallen aanzienlijk groter, dergelijke scenario's kunnen het vervolg 'gevaar' in beeld brengen.

WAT IS DE TOEGEVOEGDE WAARDE VAN DERGELIJKE RISICO SCENARIO'S?

Het mooie aan dergelijke scenario's is de combinatie tussen de bedrijfsprocessen en technische details. Denk hierbij aan het combineren van 'niet-technische' aspecten in een monitoring use case zoals hierboven beschreven. Maar ook aan het kunnen communiceren over bedrijfsrisico's met zowel technische als niet technische medewerkers. Een duidelijk beschreven scenario kan immers duidelijk maken wat bepaalde technische elementen voor risico's met zich mee brengen (e.g. een poort die open staat, kan via verschillende stappen leiden tot gestolen data met x gevolgen van dien).

Grote belang ligt echter wel in het identificeren van potentiële gevaren die zowel technische als niet technische aspecten beslaat. Er kan dan als een continu proces worden gemeten of de situatie nog in orde is.

Welke potentiele moeilijkheden zijn er wanneer risico scenario's worden opgesteld/gebruikt?

Twee potentiële lastige elementen aan deze scenario's is de mogelijke overload aan scenario's. Er zijn immers al snel heel veel manieren te identificeren hoe een hacker een bepaald doel kan bereiken. Het is lastig om een balans te vinden tussen al deze scenario's. Zaken die daarbij kunnen helpen is het identificeren van viewpoints. Een viewpoint bepaald specifieke eisen aan een scenario. Dit kan bijvoorbeeld zijn dat het een insider threat is. Of dat het een element beslaat dat alleen via interne wegen te bereiken is. Hiermee kunnen al een heleboel potentiële scenario's worden verwijderd. Daarnaast kan een externe (gespecialiseerde) partij hierbij helpen. Deze partij kan zijn ervaringen gebruiken in de selectie tussen het opstellen van scenario's.

Daarnaast is het opstellen van dergelijke scenario's ook lastig. Hier is immers zowel technische hackkennis als kennis over het IT-landschap van het slachtoffer nodig. Hiervoor kunnen Enterprise architectuur achtige overzichten van het IT-landschap worden gebruikt. Echter zijn dergelijke bestanden niet altijd voor handen. Hierbij is het wel belangrijk dat iets altijd beter is dan niets. Zonder enig overzicht van het IT-landschap is het niet mogelijk om risico scenarios op te stellen. Wanneer beperkte, of verouderde, EA-documenten worden gebruikt kan op basis hiervan de eerste analyse worden uitgevoerd. Hierna kan dan middels een soort agile werkwijze worden bepaald of de beveiliging goed genoeg is (via pen testing of red teaming kan er worden gekeken of er niet alsnog zwakheden zijn). Dit proces wisselt zich dan af met het verder uitbouwen van risico scenario's en aansterken van de verdediging.

Welke elementen wil je terugzien in een threat event om bruikbaar te zijn in de praktijk?

Het belangrijkste aan threat events binnen een scenario is dat ze gerelateerd zijn aan het IT-landschap. Ze moeten dus heel goed alignen met de situatie van het bedrijf. Hierbij moet worden gedacht aan de

verschillende connecties tussen systemen (techniek), maar ook aan de verschillende mogelijkheden van gebruikers en systemen (processen). Als dit in kaart is gebracht kan er een goede cyber risicoanalyse worden opgesteld. Hierbij is het opzetten van een 'hacker mindset' belangrijk. Wanneer hiervoor niet genoeg domein kennis is kan deze extern worden opgehaald.

HOE KAN HET DELEN VAN CYBER RISICO INFORMATIE BIJDRAGE CYBER RISICO MANAGEMENT?

Het delen van dergelijke cyber incidenten is erg waardevol en ook wel iets waar bedrijven steeds meer naar toe gaan/moeten (voorbeeld ISAC's). Echter is mondeling delen van ervaringen niet altijd genoeg. Je wil immers sneller op de hoogte blijven van wat er bij andere bedrijven gebeurt en hoe dit jou kan beïnvloeden. Een voorbeeld waar dit erg goed gaat is bij Universiteiten. Die maken gebruik van Surf als IT-beheerder en wanneer er een incident is bij een Universiteit worden details over dit incident (patroon van stappen) gedeeld met andere Universiteiten. Dit lijkt erg goed te werken, maar is nog niet te vergelijken met de commerciële wereld om de volgende redenen: Er is daar een centrale IT-provider en een centraal netwerk om deze kennis te delen. Daarnaast zijn het non-profit organisaties. Commerciële bedrijven hebben meer incentive nodig om hier tijd in te stoppen.

Het moet dus worden gefaciliteerd door een platform wil het succesvol zijn. Dit platform moet zowel het delen als het toepassen van de scenario's faciliteren. Er zal namelijk altijd een trade-off zijn tussen de kosten en baten van het delen van dergelijke kennis. Daarnaast moet er een goede balans zijn tussen de informatie die verkregen wordt en de informatie die verstuurd wordt.

Een voorbeeld wanneer informatie over een cyber incident werd gedeeld:

De politie heeft contact opgenomen met verschillende bedrijven die een vergelijkbaar profiel hadden. Er was namelijk een incident met een bepaald patroon, waarbij de kans groot was dat de daders een vergelijkbare aanval bij meerdere partijen gingen initiëren. Hier werd echter alleen kwalitatieve informatie gedeeld.

Hierbij komt meteen een belangrijk nu naar boven bij het delen van cyber gerelateerde kennis. Veel bedrijven gebruiken immers dezelfde systemen die mogelijk op dezelfde ge-exploit kunnen worden. Wanneer dit bij een bedrijf is gebeerd, kunnen andere bedrijven gewaarschuwd worden.

INTERVIEW 5

HUIDIGE SITUATIE OP HET GEBIED VAN CYBER RISICO ANALYSES

Risicoanalyses worden vanuit de business uitgevoerd. IT en security zijn ook samen een afdeling in plaats van losse afdelingen waar security een sterk controlerende houding heeft. De security aanpak is threat gebaseerd. Er wordt een grote lijst met mogelijke threats bijgehouden (en uitgebreid wanneer nodig). Op basis van deze lijst wordt periodiek gekeken welke threats relevant zijn voor de verschillende applicaties en welke controls er al wel en niet zijn uitgevoerd. Voor iedere threat wordt dan gekeken welke impact dit op de business heeft. Op basis van deze informatie wordt een baseline van potentieel risico opgesteld. Deze baseline geeft aan hoeveel risico er 'toegestaan' is. Aan de hand van de huidige securitymaatregelen kan dan worden gekeken wat er nog moet gebeuren. Er wordt hier echter wel altijd gekeken vanuit de business (wat houdt het risico in? Hoeveel kosten de securitymaatregelen? En wat is het resterende risico?). Voor nieuwe IT-projecten wordt deze baseline als requirements meegegeven. Bestaande systemen worden, zoals boven genoemd, gecheckt.

Op deze manier is een sterke preventieve security opgebouwd. De huidige focus ligt nu meer in het opbouwen van een detectieve en reactieve security. Een nadeel aan detectieve maatregelen zoals

monitoring is dat het erg lastig is om te achterhalen wat de winst hiervan is en hoeveel van deze maatregelen hiervan genoeg zijn. Denk hierbij aan securitycamera's in een bedrijf. Wat is daar de toegevoegde waarde van? Dergelijke maatregelen zijn erg lastig te kwantificeren. Daarnaast zijn dergelijke detectie maatregelen snel kostbaar aangezien ze manuren kosten (zoals bij securitycamera's iemand continu de beelden in de gaten moet houden). Daarnaast is vanuit de huidige monitoring vrij weinig naar voren gekomen. Er wordt momenteel wel gewerkt aan het implementeren van een SIEM systeem.

Naast de threat gebaseerde approach worden er ook bredere risicoanalyses uitgevoerd. Echter kosten deze analyses veel meer tijd, terwijl de andere approach vaak al voldoende is.

HOE KUNNEN RISICO SCENARIO'S IN DE PRAKTIJK GEBRUIKT WORDEN?

Een belangrijk en waardevol aspect waar dergelijke scenario's kunnen worden gebruikt is de communicatie tussen de business en security mensen. Op die manier kan je beter het belang over brengen van bepaalde securitymaatregelen. Door scenario's te betrekken kan er een duidelijke link tussen de maatregelen en potentiële gevolgen worden weergegeven.

Daarnaast worden er impliciet wel dergelijke scenario's gecreëerd tijdens risicoanalyses. Er wordt dan met een team gekeken naar een bepaalde applicatie. Om tot de risico's van die applicatie te komen wordt er gekeken naar wat voor soort aanvaller een dergelijke applicatie zouden willen aanvallen en hoe ze dat dan zouden doen. Dit proces wordt echter niet expliciet uitgevoerd.

Een belangrijk aspect van zo'n scenario gedreven methode is dat je creatieve en nieuwe risico's ontdekt, ipv blijft steken bij de standaard risico's uit checklijsten. Het motiveren van creatief denken moet dan ook erg worden beloond. Een voorbeeld hierbij is dat een huis erg goed kan zijn beveiligd met stalen deuren en tralies voor de ramen, maar dat de niet standaard manieren (schoorsteen, kelder, of door de muur) dan vaak worden vergeten. Een aanvaller kan dan dus nog steeds binnen komen. Echter kost het opstellen van dergelijke risico's wel erg veel tijd en levert het niet voor iedere applicatie een meerwaarde op. Een betere manier zou dan zijn om deze aanpak te combineren met een gestructureerde threat based assessment. Aan de hand van zo'n algemene en snellere methode kan worden bepaald waar de grootste risico's (voor het gehele bedrijf) liggen en waar dus een diepere analyse nodig kan zijn.

WAT IS DE TOEGEVOEGDE WAARDE VAN SCENARIO'S IN EEN RISICO ANALYSE?

Wat nodig vanuit risicoanalyse?

Een risicoanalyse moet gericht zijn op de business. Hiermee wordt gedoeld op het identificeren van potentiële impact op de business. De potentiële impact bepaalt de mate van control. Deze business focus is belangrijk om de beveiliging niet alleen als een beperking te zien, maar ook te zien als waarde. Daarnaast is het soms nadeliger voor een bedrijf om een risico te controleren, dan te accepteren. (Dit kan financieel zijn door de hoge kosten, maar het kan ook komen doordat de maatregelen bedrijfsprocessen stoppen).

Moeilijkheden opstellen scenario's?

Het lastigste met het opstellen van dergelijke scenario's is de hoeveelheid aan tijd die het kost om ze op te stellen. Dergelijke risicoanalyses zijn veel tijdsintensiever, het is dus niet voor iedere applicatie rendabel om dit uit te voeren. Er zal dus een combinatie moeten komen tussen meer gestandaardiseerde methoden en meer uitgebreide methode zoals deze scenario gebaseerde manier.

HOE KAN HET DELEN VAN CYBER RISICO INFORMATIE BIJDRAGE CYBER RISICO MANAGEMENT?

Cyber incidenten bij een bedrijf geven ook de zwakheden weer. Hier moet dus vertrouwelijk mee om gegaan worden. Om deze reden is het belangrijk een goede vertrouwensband op te bouwen. Wanneer dit niet het geval is, zal er ook geen waardevolle informatie worden gedeeld. Binnen een bepaalde community kan zo'n band goed worden opgebouwd. Er moet dan wel een balans blijven tussen hoeveel input iedereen geeft.

Een ander punt wat nadelig kan zijn voor het delen, is de mogelijkheid tot verschillende belangen. Zo kan het nadelig zijn om (potentiële) klanten te vertellen over alle cyber incidenten die bij jou hebben plaatsgevonden.

Een oplossing voor bovenstaande problemen is het delen van anonieme informatie. Echter wordt de informatie wel minder waardevol zonder specifieke context. Een manier hoe dergelijke informatie wel nog waardevol kan zijn is als het automatisch verwerkt en gedeeld wordt met degene voor wie het relevant is (voorbeeld Watson die zelf cyber incidenten analyseert). Dit systeem kan dan als anonieme en betrouwbare tussenpersoon fungeren.

Wat wil je zien vanuit gedeelde cyberinformatie?

Drie informatieelementen zijn belangrijk om keuzes om te ontvangen, en naar te handelen. Dit is informatie over de high-level ontwikkelingen in het gehele cyber threat landschap. Informatie over acute en relevante dreigingen, en als laatste gekwantificeerde informatie over risico's vanuit een grote populatie.

INTERVIEW 6

CURRENT SITUATION IN CYBER RISK MANAGEMENT

The focus of the risk analysis, and cyber security team is towards prevention and detection. Much of the analysis is based on the experience and knowledge of the employees that conduct the analysis. The output is therefore dependent on the experience of the employee as well. One of the reasons why the output is dependent on the employee who performs the analysis, is that there is no standardized approach of a complete cyber risk analysis within the organization.

They do use frameworks (e.g. ISACA ISF ISO) as guidelines. These frameworks merely provide some structure and guidelines to check the vulnerabilities within the organization. There is not a complete methodology to perform the approach.

They do make use of some cyber intelligence sources, the information that is mostly valuable include technical details, operational implications, and TTP information (tactics, techniques, and procedures).

HOW CAN RISK SCENARIOS BENEFIT THE RISK ANALYSIS?

The scenarios would provide a good overview of the potential cyber risks. The taxonomy could guide as a guideline for the information that should be identified during the analysis. Once they are identified they could have been mapped together in a complete cyber risk scenario. It should be adaptable to the needs of an organization. The structure should therefore be open for change (besides the specific needs, will the needs of such a taxonomy change alongside the developments of the cyber threat landscape). Besides the ability to change, it should be possible to identify a scenario with the taxonomy without too much information about the occurred incident.

Another important aspect for adaption of such a methodology within a large organization, is the time the organization needs to change its overall approaches.

Important aspects of a taxonomy to capture cyber risk scenarios are:

- Threat agent (more about his resources than providing a label)
- Threat events
- Vulnerabilities
- Sources that were used by the threat agent
- Which asset is attacked
- What kind of methods were used?
- TTP details (this is however not perse needed in a scenario):
    - Domain name of the malicious host
    - IP addresses that should be blocked
    - Entry points
    - etc

How van cyber risk knowledge sharing benefit a risk analysis?

A complete scenario would provide a good overview of the entire risk once it has been shared. The contextual factors that are included to keep the risk within its context.

An important aspect for knowledge sharing to become successful is that a win-win situation is created. Another possibility is a legal obligation (such as the Wet meldplicht datalek in the Netherlands).

An ideal situation for knowledge sharing would be, if a third party would arrange it. This party should organize the sharing practices, but also check and sanitize the scenarios where needed.

The stakeholder that receives the knowledge should be taken into account. A C level person would for instance like a tactical overview of the scenario. This should not include too much details. But a more technical cyber security oriented employee would like more details, especially about the part of the scenario where he is responsible for.

The quantification of probability values would be difficult. Some estimation could be made, but they are still based on the judgements of some experts. For this reason it is questionable if a complex quantifiable method would be of an added value, over a more qualitative and simpler method. In other words: would the extra effort of a complex quantified method result into better results? Given the judgmental input of the models.

H. CATEGORIZATION WITHIN THE DELOITTE CYBER CASE REPOSITORY

Table elements	Example data
Organization	*A large retailer that sells a variety of food and non-food products.*
Industry	*Retail*
Company name	*Confidential*
Affected Information Asset	*Financial information*
Timeline	*Q4 2013*
Attacker Category	*Cyber criminal*
Scenario	*Malware was installed on a point-of-sale system. This malware recorded the credit cards and PINs, and was able to spread itself throughout the company.*
Attackers and motivation	*Financial gain (by selling the gathered credit card information).*
Techniques used	*Malware (which was for sale on the criminal market).*
Business Impact	*The companies brand was damaged which decreased the sales. A drop of the share price, heavy fines, and the cost to monitor the (possibly) affected credit cards resulted.*