Master thesis

Dealing with uncertainty: cybersecurity risk assessment approaches

A qualitative research on cyber risk assessment practices in organizations

Universiteit
Leiden
Governance and Global Affairs

Executive MSc Program Cyber Security 2019/2020

Author	Kees Mastwijk
Student number	S2444550
Date	30 December 2020
Supervisors	Dr. James Shires, Dr. Tatiana Tropina

Acknowledgements

This thesis concludes a two-year journey of the Executive Master Cybersecurity. The journey has broadened my understanding of the different disciplines of cybersecurity in many ways. I would like to thank all (guest) lecturers for the inspiring lessons, the Cyber Security Academy and Leiden University for facilitating, as well as my fellow students for exchanging ideas, thoughts and collaboration.

I wish to thank all the interviewees who took part in the research for their valuable input and sharing their experiences. This research would not have been possible without their help. A special thank you to my employer Vest for stimulating me and giving me the opportunity to do this master.

I would especially like to thank my family for supporting me during this journey. Thank you also for the patience and understanding for studying late in the evening, sometimes very early mornings and weekends.

Last but not least, I would like to express my gratitude and appreciation for my two thesis supervisors, Dr. James Shires and Dr. Tatiana Tropina, for their continued support and guiding me into the right direction.

Abstract

Digitalization adds convenience to our lives in many ways. We communicate and do shopping online, turn the heating up at home while leaving the office, and connect the lights to remote control them from the couch. The examples illustrate how technology has shaped our lives in the past decades. Our interaction with technology has changed dramatically.

This development affects organizations as well. Organizations adopt new technologies to service their clients in order to gain competitive advantage. Processes and services are offered digital and in many cases, online. Independent of the processes and services offered, organizations require adequate security measures to protect their assets. As examples in the news illustrate, not doing so may result in serious business impact like loss of reputation, financial losses, operational or legal impact, or even worst case scenarios like bankruptcy.

At the same time, there are numerous challenges that organizations face in securing their assets. These challenges include a rapid changing threat landscape, new technologies, vulnerabilities in software, and the strongly interconnected and inherent complex nature of the cyber domain. To what extent are organizations able to protect their assets against cybersecurity threats? How do organizations assess their cybersecurity risks? Do these approaches fit the current cybersecurity challenges? Identifying, analyzing and evaluating cybersecurity risks can become a daunting task. Fortunately, there are many risk frameworks, methods and techniques available that organizations can adopt. Maybe even that many that selecting a fit for purpose approach becomes daunting by itself.

This qualitative research explores the current state of cybersecurity risk assessment practices in organizations by researching to what extent the available cybersecurity risk assessment methods and techniques actually have been adopted by organizations. Second, the research investigates whether the chosen approach caters for the challenges in the cyber domain, and what benefits and limitations are perceived.

Keywords: cyber risk | cybersecurity | uncertainty | risk assessment

Table of content

1 Introduction

1.1 Context and relevance of research

Cybersecurity is becoming an increasingly important topic for organizations. As digitalization continues and new technologies are adopted in a rapid pace, organizations heavily rely on information technology. Protecting against cybersecurity risks has become a critical factor for many organizations (Wang, Neil, & Fenton, 2020). Cybersecurity risk assessments play an important role in preventing and mitigating cybersecurity risks. Risk is referred to by as 'the possibility of an event which would reduce the value of the business were it to occur (Blakley & Mcdermott, 2001). An event like this is referred to as an adverse event. Risk assessments can help organizations to identify threats and prioritize on the biggest concerns (Peltier, 2005).

Organizations that are hit by data breaches, disruption, cybercrime and hacking hit the news on a daily basis. Many will argue that it is not a question if a cybersecurity incident will hit an organization because it definitely will, the questions should be when it will happen. The number of threats and capable adversaries is growing faster than defense mechanisms we can think of and implement. Some examples of cyber risks organizations are facing include sabotage by competitors, denial of service attacks by hacktivists, transferring of funds by criminals, and nation states launching attacks on foreign companies (Hiller & Russell, 2013).

As organizations rely on technology more and more, dependency is growing and the need for securing digital environments increases. It is no longer only the traditional information technology (IT) environment that is processing personal, sensitive or confidential data that needs to be protected. As the cyber and physical domain converges, the need to protect operational technology (OT) against disruption increases as well. Cybersecurity incidents may result in different types of business impact, ranging from financial, reputational, legal and operational losses. On top of that, OT adds safety risks to the risk landscape.

The complexity and interdependency of information systems increases. The rapid pace of technology is another factor that complicates the cyber domain. For example, the Internet of Things (IoT) adds another layer of interconnectivity to the cyber domain. Till date, little data is available on the number of cyberattacks, hacks, data breaches, and the amount of disruption. Although it may be doable to determine the potential impact of these cyber risks, determining the likelihood of these risks is a rather difficult exercise due to the absence of these numbers.

Fortunately, many approaches have been developed in the past for assessing risks. For example, the international standard ISO31010 (International Organization for Standardization, 2019) lists thirty-one tools and techniques that can be used for assessing risk. They range from brainstorming, check-lists, scenario analysis, business impact analysis to bow tie analysis, to name a few. The standard is independent of the type industry of the organization.

More specific to cybersecurity, the Trespass project (Trespass Project, 2014) identified and analyzed eighteen risk assessment methods, as well as four information security risk assessment standards.

The way organizations assess, i.e. identify, analyze and evaluate, cybersecurity risks is assumed to be dependent on a number of factors. First of all, the reason why organizations engage in cybersecurity risk assessments is likely to influence the choice for a risk assessments methodology. We can think of several reasons, including meeting regulatory requirements, peer pressure, meeting compliance requirements, as well as requirements from cybersecurity insurance companies.

Depending on the industry, regulators are likely to require some form cybersecurity risk assessment. For example, the European Central Bank monitors how banks manage their cybersecurity risks (European Central Bank, n.d.). In the Netherlands, the Dutch National Bank (DNB) sets requirements for financial institutions with regard to cyber risk assessment and management (De Nederlandsche Bank, 2020). The latter requires financial institutions to periodically perform IT risk assessments on a regular basis and to include up-to-date cyberthreats in assessments.

Organizations may as well be forced to conduct cybersecurity risk assessments by peers. For example, organizations may require a vendor to perform such assessments to get assurance on the service the vendor delivers. The format, techniques and methods used by the vendor may vary, as long as it fits the client’s expectations.

Meeting compliance requirements may be a third reason for organizations to perform cybersecurity risk assessments. One obvious compliance requirements is applicable for organizations that have an Information Security Management System in place as described in the ISO27001 standard (International Organization for Standardization, 2013).

Additionally, the security maturity level of the organization is likely to influence the cybersecurity risk assessment techniques and methods adopted. It is assumed that organizations with a higher security maturity level will have a more advanced cybersecurity risk assessment process in place compared to less mature organizations.

Finally, the available resources in an organization with knowledge and expertise with regard to cybersecurity risk assessments will be relevant to take into account when it comes to choices made in risk assessment techniques and methods.

Given the challenges regarding the complexity of cyberspace, as well as the many choices an organization can make in the selection of cybersecurity risk assessment approach, this research explores how organizations deal with the challenge of assessing cybersecurity risks. The research first describes to what extent organizations use the available cybersecurity risk assessment approaches. Next, the research explores the reasons for organizations to adopt a certain approach, or not.

1.2 Problem description

A theoretical framework was created for this research consisting of the hypothesis that organizations are facing challenges in assessing (identifying, analyzing and evaluating) their cybersecurity risks due to the wide variety of available cybersecurity risk assessment methodologies and their respective differences. The second hypothesis in this research is that the current methodologies do not cater for the challenges in the cyber domain, resulting in unreliable assessment results and, as a consequence, uninformed decision making.

1.3 Objectives of the study

The main objective of this study is to identify how organizations are assessing cybersecurity risks, what the benefits and limitations of these approaches are, and what improvements can be made to current cybersecurity risk assessment techniques and methods. In order to do so, the research takes a descriptive approach with regard to identifying the cybersecurity risk assessment frameworks, techniques and methods used by organizations. Second, the research takes an explanatory approach with regard to the 'why' part of selection of these approaches by organizations. This latter part of the research aims to determine what the rationale is for organizations to (not) select a framework, technique and/or method.

Assessment in this paper is defined as the *identification, the analysis and the evaluation of cybersecurity risks*, as defined in the international information security risk assessment standard ISO27005 (International Organization for Standardization, 2018). As organizations can have different reasons to perform cybersecurity risk assessments, we will explore *why* organizations perform cybersecurity risk assessments. The rationale for cybersecurity risk assessments is likely to influence the choices for techniques and methods used for assessments.

Next, the research analyzes to what extent cybersecurity risk assessment results are integrated in an organization wide risk profile, and how evaluation of risk assessments is performed. Finally, the research provides input for possible improvement areas in the field of cybersecurity risk assessments as we aim to identify the pros and cons of current cybersecurity risk assessment techniques and methods.

1.4 Research questions

The main research question of this study is:

"To what extent do organizations use available cybersecurity risk assessment techniques and methods, and what is the reason for (not) selecting them?"

This research contains both a descriptive as well as an explanatory part. The first part of the research question refers to the descriptive part and aims to identify the use of cybersecurity risk assessments within organizations. The second part of the research question aims to explain the reasons why organizations have adopted certain cybersecurity risk assessment approaches or why not.

In order to be able to answer the main research question, the following sub-questions were created:

RQ 1 - What cybersecurity risk assessment techniques and methods are there?

Organizations can choose from a wide variety of approaches with regard to cybersecurity risk assessments. This research question explores the available frameworks, techniques and methods that organizations can adopt, and is performed by means of literature review.

RQ 2 – What factors should be considered when selecting a cybersecurity risk assessment approach?

As there are many approaches to cybersecurity risk assessment, it makes sense to think of relevant factors before adopting a certain approach. What are these relevant factors to consider? This research question will be answered by means of literature review.

RQ 3 – Why do organizations perform cybersecurity risk assessments?

Although the answer to this question may seem obvious in the sense that cybersecurity incidents should be prevented, there are other reasons that could be considered. For instance, regulators may require organizations to perform cybersecurity risk assessments according to a predefined method or framework. Compliance requirements may instruct organizations to perform assessments as this is the case with ISO27001 certified organizations. Peer pressure can also play a role in the relation between an organization and customers, where customers request the organization to share information on the risk assessments performed. The reason for performing cybersecurity risk assessments may for that reason differ and influence the choice for a certain risk assessment approach. This research question will be answered by means of interviews.

RQ 4 - What cybersecurity risk assessment approaches do organizations take?

To what extent do organizations actually use the available cybersecurity risk assessment approaches? Have they adopted one or more of these frameworks, techniques and methods? This research question will be answered by means of interviews.

RQ 5 – What limitations and benefits are recognized with regard to the adopted cybersecurity risk assessment approach?

How does the adopted cybersecurity risk assessment approach cater for the needs of the organization? What benefits does the approach bring, and what limitations are recognized? Specific attention will be paid to the ability of the selected approach to integrate with other types of business risks. As part of this research question we aim to identify potential improvement areas for the cybersecurity risk assessment practice. This research question will be answered by means of interviews.

1.5 Scope of research

This research focusses on cybersecurity risk assessment approaches within both public and private sector organizations. For the purpose of this research, risk assessment is defined and scoped as the activities needed for risk identification, analysis and evaluation. For that reason, the research is limited to organizations that have at least one of those risk assessment activities in place.

Out of scope are risk management activities not being part of the risk assessment process. These activities include establishing the context and risk treatment. Refer to paragraph 2.2 for more information on the different risk management activities.

1.6 Academic and social relevance

Many research has been done on cybersecurity risk assessments, including (Trespass Project, 2015), (Cherdantseva et al., 2016), (Pan & Tomlinson, 2016), (Labunets, 2016), (Ganin et al., 2020). The main focus of these studies is related to the available security risk assessment techniques and methods, their pros and cons, on their effectiveness and ease of use.

This qualitative research builds on the current studies and further explores the topic of cybersecurity risk assessment practices used by organizations. This explanatory focused research aims to provide a current state of affairs with respect to cybersecurity risk assessment approaches adopted by organizations, including the reason why organizations conduct cybersecurity risk assessments, what techniques and methods are used, what the perceived benefits and limitations of the chosen approaches are, and what improvements could be made to the current cybersecurity risk assessment practices. By doing so, this research aims to bridge gaps between literature on cybersecurity risk assessment approaches, and practice by collecting empirical evidence. This way, the research will provide in guidance on further cybersecurity risk assessment research and improvements.

1.7 Thesis outline

This paper is structured as follows. Chapter one contains an introduction on this research, and elaborates on the objectives and research questions. Chapter two contains the results of the initial literature review that has been performed. Relevant literature with regard to (cybersecurity) risk management and assessment, frameworks, techniques and methods was analyzed. The research methodology and design was developed based on the literature review and is described in chapter three. Chapters four, five and six contain the analysis and results from the empirical data. Chapter seven contains a conclusion, chapter eight contains a reflection on this research and possible future research. The chapters that are related to the main research questions (chapters two, four, five and six) start with the research results, followed by a discussion paragraph with the key findings and synthesis.

2 Literature review

2.1 Cybersecurity risk management conceptualization

For the purpose of this research, we need to conceptualize the field of cybersecurity risk assessments. In this paragraph, we take a closer look at the term ‘cyber’ as well as risk assessment and management.

In the past decade, the terms cyberspace and cybersecurity have gained popularity. What exactly do those terms mean, and do they differ from the well-known information or IT security? In this research we use the definition that is referred to in the model that Van den Berg introduced: ‘*cyberspace concerns the space of cyber activities as executed by people while making use of ICT systems’* (van den Berg, 2017). This model consists of three layers of cyberspace, i.e. the technical layer, the socio-technical layer and the governance layer. The technical layer comprises the technology services, securing this layer is referred to as IT-security. The socio-technical layer focusses on the interaction between people and technology; this layer concerns all activities and behavior of people using (complex) technology. Securing these cyber activities is referred to as cybersecurity. The governance layer deals with acceptable risk levels and compliance topics within the two aforementioned layers.

The ambition to control uncertainty is paradoxical by nature (Power, 2004). After all, we can’t control things we don’t know. However, there is growing need to forecast and calculate uncertainty. Power identified the shift in the mid-1990s from an internal control mindset to a risk management mindset (Power, 2004). Power refers to this ambition to control as ‘the risk management of everything’. The benefit from being able to calculate risks more accurately is better decision making. In his book, Power also explains the creation of the concept of ‘operational risk’. An important driver for the concept was the collapse of the Barings bank. Organizations felt the need to get a grip on these kinds of disastrous events. The Basel committee, as the global supervisor for financial institutions, created the Basel framework, a framework in which organizational dangers and uncertainties are collected. The framework has been updated since, currently the Basel 2 standard is effective. The Basel 2 standard includes seven categories of loss event types: (i) internal fraud, (ii) external fraud, (iii) employment practices and workspace safety, (iv) client, products & business practices, (v) damage to physical assets, (vi) business disruption and system failures, and (vii) execution, delivery & process management (Basel Committee on Banking Supervision, n.d.). For financial institutions, adopting this standard is best practice as reporting on those categories is required by regulators. Cybersecurity risks are considered to be one of the operational risks, among all other types of risks an organization may face. Within the Basel 2 standard, cybersecurity events may be mapped to the external fraud category (Basel 2 level one). This category contains events related to systems security (Basel 2 level two), for example hacking damage and/or theft of information (Basel 2 level three). Although not described in detail, the Basel standard demonstrates how cybersecurity risk events can be mapped to operational business risk categories.

The concept of risk assessment was well explained by Kaplan and Garrick (Kaplan & Garrick, 1980). The authors argued that risk assessments should answer three main questions:

- What can happen? (i.e. what can go wrong?)
- How likely is it that that will happen?

- If it does happen, what are the consequences?

Although the concept dates from four decades ago, it is clear that those questions are in essence exactly what cybersecurity risk assessments should entail. Next steps should of course include decisions on a risk treatment strategy, like accepting, mitigating, and transferring risks. However, for this research those steps are not in scope since they are part of the subsequent steps in the risk management process.

Researchers have proposed improved versions of these three aforementioned basic risk question, for example replace the question by questioning if there are better risk management policies available (what can go wrong), how probable each of one's next actions should be (likelihood), and would a different choice of policy give me lower regret given the uncertainties (impact) (Cox, 2012).

The three above mentioned basic risk assessment questions seem easy to answer. Within the context of the cyber domain we should however take into account complexity as an important factor. Van den Berg et al. (van den Berg et al., 2014) explained the technology developments in a precise manner. Going back to the early days of cyberspace, there was a strong focus on securing the technical layer, and information in particular. Confidentiality, integrity and availability, also referred to as the CIA triad, were the pillars of information security.

Van den Berg argues that cyberspace has developed from a technical domain to a more socio-technical domain, in which actors in cyberspace are interacting with the technical layer. This development has led to the Internet we know now, the 'hyper-connected world' (Helbing, 2013), or highly interconnected cyberspace. Within this context of highly interconnected systems, the risk of possible cascading effects should be taken into account as well. Cyber ecosystems become more susceptible to cascading effects when the number of interconnections grows. Pescaroli argued that interdependencies and vulnerabilities are important factors to consider when reducing risks related to cascading effects (Pescaroli & Alexander, 2015).

2.2 Assessing risk

The term risk assessment refers to one of the steps in the risk management process. In order to have a common understanding of the term risk assessments, we refer to the definition used by the International Organization for Standardization (International Organization for Standardization, 2018). ISO releases standards which are recognized as industry best practices, and has released multiple standards on information security, risk management and information security risk management (hereafter ISO series on information security). According to ISO, the process of assessing risks includes (i) the identification of risk, (ii) the analysis of risk and (iii) the evaluation of risk. Risk assessments are part of the risk management process. Figure 1 shows the risk management process, and depicts the risk assessment components.

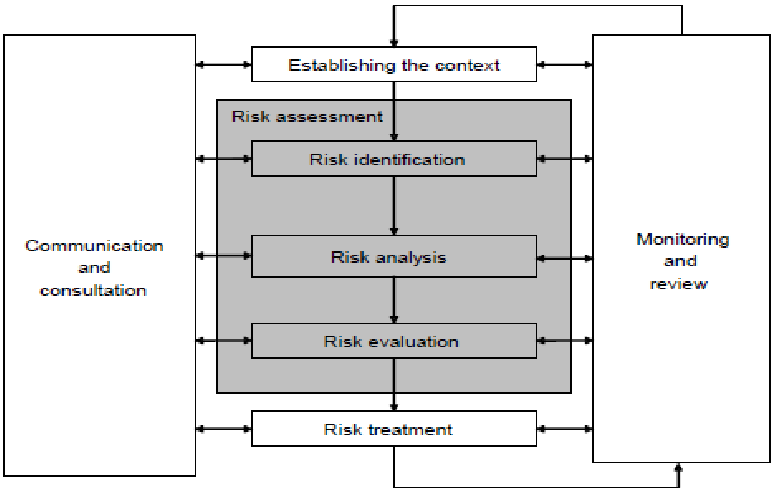


Figure 1 - Risk assessment process according to ISO27005

Risk identification is the phase of risk assessment in which possible scenarios are identified. Risk scenarios are built by taking into account the relevant 'ingredients'. According to the ISO27005 standard, these ingredients include the identification of assets, threats, existing controls, vulnerabilities, and consequences.

Risk analysis refers to the phase in which the level of risk is determined. This is done by assessing the consequences and by assessing the incident likelihood. The ISO27005 standard states that a risk analysis methodology can be *quantitative* and/or *qualitative*, i.e. assessing consequences, incident likelihood and the level of risk identification can take a quantitative or qualitative approach. The standard describes the differences between these approaches. In general, it can be stated that qualitative risk assessments are used for high-level risk assessments where an indication of risk in terms of high, medium or low is sufficient. A qualitative approach is often easy to adopt. On the other hand, a quantitative approach is more suitable for assessments requiring detailed results. A quantitative approach is for that reason more complex and expensive. More information on qualitative and quantitative risk assessments is included in paragraph 2.3.3.

Risk evaluation is the third and last phase of risk assessment. Evaluation of the risk scenarios and their respective levels of risk are evaluated against the risk acceptance criteria.

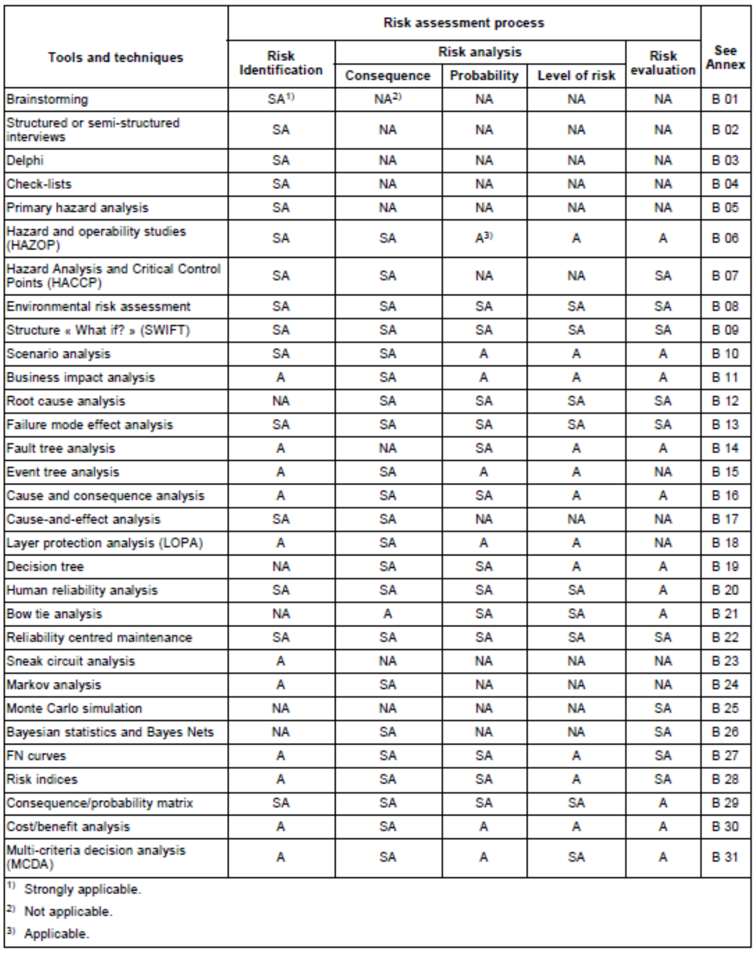
2.3 Cybersecurity risk assessment frameworks, techniques and methods: an overview

Lots of research is done on identifying, analyzing and comparing cybersecurity/IT security risk assessment techniques and methods. Literature review shows that many ways exist to assess cybersecurity risks. Approaches vary from using lists and catalogues of threats and controls, to more advanced ways of risk assessments like threat modeling and threat profiling.

A cybersecurity risk assessment approach may be referred to as a framework, standard, technique and/or a method. A framework refers in this paper to a complete risk management framework, in which a risk assessment approach is included.

2.3.1 Generic risk assessment methodologies

A source of risk assessment techniques and methods can be found in the ISO standard ISO IEC 31010:2019 Risk management — Risk assessment techniques (International Organization for Standardization, 2019). This standard provides guidance on general risk assessment techniques and is not limited to a specific domain. It categorizes risk assessment techniques into categories. Some risk assessment categories listed in the standard are look-up methods (check-lists and preliminary hazard analysis), supporting methods (structured interview and brainstorming, Delphi technique), scenario analysis (root cause analysis, scenario analysis, business impact analysis), and controls assessment. It is argued that this standard is relevant to the research as it contains techniques used for cybersecurity risk assessments like the use of check-lists, interviews and brainstorming, scenario analysis, business impact analysis, bow tie analysis, and layers of protection analysis. Figure 2 contains the overview of risk assessment tools and techniques as listed in ISO31010.



Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1]	NA[2]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1] Strongly applicable.

[2] Not applicable.

[3] Applicable.

Figure 2 - ISO31010 risk assessment tools and techniques

2.3.2 Cybersecurity risk assessment methodologies

An initial overview of security risk assessment methods was identified in the Trespass project. The project was performed by the European Commission funded Trespass Project and researched available information security risk assessment standards, methods and tools (Trespass Project, 2015). The project identified nearly twenty different methods for risk assessments, including Coras, Cramm, Fair, IRAM, and Octave.

The EU funded Trespass project created an overview of security risk assessment methods (Trespass Project, 2014). Contrary to the ISO31010 standard, the Trespass project focused on methods instead of techniques.

The rise of new technologies also introduced an increased need for tailored cybersecurity risk assessment approaches. For example, cybersecurity risk assessment frameworks were developed for Internet of Things (IoT) environments. As existing risk frameworks could not be easily adapted to IoT specific risks, research was done on the of applicability of those frameworks for IoT (Kandasamy, Srinivas, Achuthan, & Rangan, 2020).

Another example of specific cybersecurity risk assessment frameworks was created for SCADA (Supervisory Control And Data Acquisition) environments. In their study, Cherdantseva et al. examined twenty-four cybersecurity risk assessment methods in the context of SCADA systems (Cherdantseva et al., 2016). The authors rightfully state that many SCADA specific risk assessment methods are derived from traditional IT security risk assessments. However, due to the characteristics of SCADA systems, those methods need adjustment to meet the requirements of the OT environments.

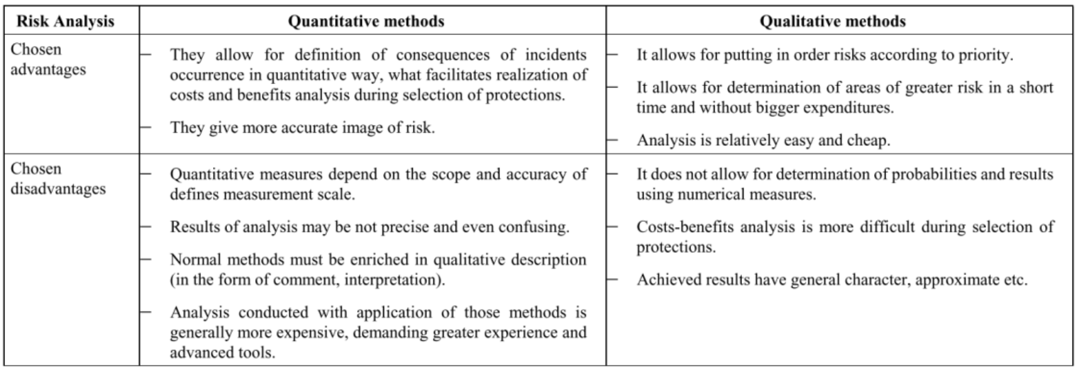
Finally, a more advanced category of cybersecurity risk assessment techniques is worth mentioning. Threat modeling is a way of threat identification which is usually used in a software development environment. Examples of threat modeling include STRIDE, CORAS, attack trees, and abuser stories (Hussain, Kamal, Ahmad, Rasool, & Iqbal, 2014). A threat modeling methodology that gained more attention in the recent years is the MITRE Att&ck framework (MITRE, n.d.).

In 2018, the National Institute of Standards and Technology (NIST) published the latest version of the Cybersecurity Framework (NIST, 2018). This framework categorizes cybersecurity practices in five domains: Identify, Protect, Detect, Respond and Recover. Each domain contains a number of controls that an organization can implement. As such, this NIST framework can be considered to be a checklist for the implementation of relevant cybersecurity controls. Next to these controls, the framework also offers so called ‘tiers’ of cybersecurity. Although NIST does not refer to those tiers as maturity levels, the tiers do describe a ‘an increasing degree of rigor and sophistication in cybersecurity risk management practices’ (NIST, 2018). Each of the four tiers include a level that could be selected on the topic of: (i) risk management, (ii) integrated risk management program, and (iii) external participation.

2.3.3 Qualitative and quantitative risk analysis methods

Next to differences in the process steps of a risk assessment methodology, there are two important different ways of analyzing risks. Risk assessments can be conducted by means of a qualitative or quantitative method. In this paragraph we take a closer look at both approaches.

The main difference between both approaches is the way of expressing risk values. Qualitative approaches present risk assessment results in a descriptive way, and quantitative approaches express risk values in a numerical way (Rot, 2008). Bialas captured the main differences as shown in figure 3.



Risk Analysis	Quantitative methods	Qualitative methods
Chosen advantages	– They allow for definition of consequences of incidents occurrence in quantitative way, what facilitates realization of costs and benefits analysis during selection of protections. – They give more accurate image of risk.	– It allows for putting in order risks according to priority. – It allows for determination of areas of greater risk in a short time and without bigger expenditures. – Analysis is relatively easy and cheap.
Chosen disadvantages	– Quantitative measures depend on the scope and accuracy of defines measurement scale. – Results of analysis may be not precise and even confusing. – Normal methods must be enriched in qualitative description (in the form of comment, interpretation). – Analysis conducted with application of those methods is generally more expensive, demanding greater experience and advanced tools.	– It does not allow for determination of probabilities and results using numerical measures. – Costs-benefits analysis is more difficult during selection of protections. – Achieved results have general character, approximate etc.

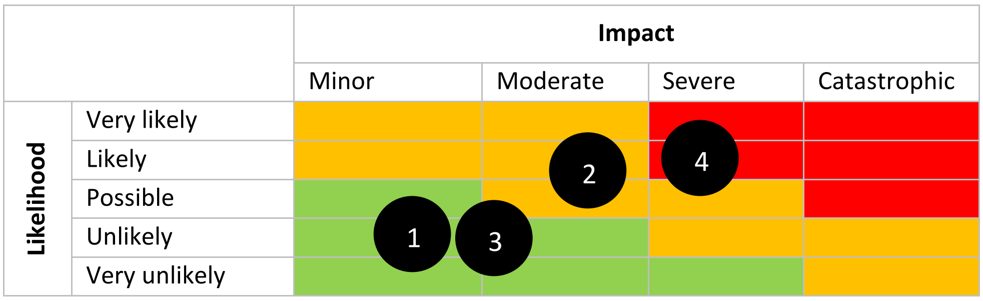
Figure 3 - Comparison quantitative and qualitative risk assessments. Reprinted from (Bialas, 2006)

The definition of qualitative risk analysis according to the ISO series on information security is: *'Qualitative risk analysis uses a scale of qualifying attributes to describe the magnitude of potential consequences (e.g. low, medium and high) and the likelihood that those consequences will occur.'* (International Organization for Standardization, 2018).

Examples of qualitative risk management methodologies include COBIT, ISO/IEC 27005:2011, SARA, Octave, CORAS, while examples of quantitative risk management methodologies include ISRAM, CVRAMM, BSI and CORA (Ruan, 2017).

In their paper, Pasman, Rogers and Mannan explained how risk assessments evolved over time (Pasman, Rogers, & Mannan, 2017). As the authors state, the basis for many of current risk assessment methodologies was borrowed from the nuclear community. In its early days, much of the developed methodologies were qualitative by nature using red, orange and green as indicators for risk, as this is still the methodology used in many industries. However, over time, semi-quantitative methodologies were developed by actually estimating probability and consequences. Later, regulatory requirements forced organizations to perform full quantitative risk assessments with detailed analysis in order to obtain a license for operating a plant (Pasman et al., 2017).

According to the ISO series on information security, a qualitative risk assessment approach can be beneficial for obtaining a first, high-level overview of risks. The approach is considered to be less complex and less costly compared to quantitative approaches. The most commonly used qualitative approaches are using scales, for example a scale with a high, medium and low values, or a scale with values from one to five, and assign these values to an estimated likelihood and impact of a certain risk. The risk is then calculated by multiplying the likelihood and impact values. This way, a prioritized list of risks can be obtained and/or plotted on a risk heatmap. An example of a risk heatmap, or risk matrix, is illustrated in figure 4.



		Impact			
		Minor	Moderate	Severe	Catastrophic
Likelihood	Very likely	🟧	🟧	🟥	🟥
	Likely	🟧	🟧 2	🟥 4	🟥
	Possible	🟩	🟧	🟧	🟥
	Unlikely	🟩 1	🟩 3	🟧	🟧
	Very unlikely	🟩	🟩	🟩	🟧

Figure 4 - Risk heatmap or risk matrix example

This example of a risk matrix gives some guidance in risk treatment options, visualized by colors. The risks in the green part of the matrix (risks one and three) have an acceptable level of risk: there is a low impact and low likelihood for these risks. Risks plotted in the orange part of the matrix (risk two in the example) needs attention as the likelihood of the risk is set to likely with a moderate impact. Finally, risk four is likely to happen and has a severe impact value.

Although widely used and adopted, qualitative risk analysis is also criticized. For example, Hubbard and Seiersen wrote about problem areas in the field of qualitative methods (Hubbard & Seiersen, 2016). Problems include the misunderstanding of people when applying the qualitative descriptions of likelihood. I.e. one should describe the values, or levels, properly, but even when deliberate steps are taken to standardize these values of likely, possible, highly likely, they remain misunderstood.

A quantitative risk analysis is defined by ISO as '*Quantitative risk analysis uses a scale with numerical values (rather than the descriptive scales used in qualitative risk analysis) for both consequences and likelihood, using data from a variety of sources.'* (International Organization for Standardization, 2018).

According to the ISO series on information security, quantitative risk assessment approaches can be helpful to further analyze the biggest risks identified in the qualitative risk assessment.

Hubbard and Seiersen argue that often excuses are used for not adopting quantitative risk assessment methods. These excuses include complexity, the lack of data, unpredictable human error, and rapid changing technology (Hubbard & Seiersen, 2016). It is noticed that exactly these factors are recognized in literature as the challenges in cybersecurity risk assessments as we will identify in paragraph 2.6. The authors advocate that quantitative risk assessment methods do a better job in determining risk levels and ultimately, better decision making. The authors argue that there is often more useable data available then we think, and quantitative methods require less data then we assume.

Recently, a quantitative cybersecurity risk assessment methodology was proposed by Wolthuis and Philipson (Wolthuis & Phillipson, 2019). In their paper, the authors argue that current risk management and assessment practices, mainly performed in a qualitative way, do no longer cater for business needs.

The authors also argue that qualitative risk assessments have important disadvantages. These include the dependance on the expertise of staff, the frequency of these assessments, and an often used asset based risk assessment approach. Next to that, qualitative risk assessment results rely heavily on the definition of the risk levels. A second drawback is that the risk levels often do not have enough distinctive power. I.e. when using risk scales of like high, medium and low, there is a big chance that the majority of the risks will end up with a medium score. The methodology that Wolthuis and Phillipson propose use a Bayesian Belief Networks model and quantifies the likelihood part of a risk. A proof of concept was performed to test this model. Using the scenario of a Distributed Denial of Service attack as a threat example, the methodology was tested in cooperation with several banks. Core elements in the model include 'nodes', which can be considered relevant risk factors, and probability tables. This input was used to build the example model as shown in figure 5.

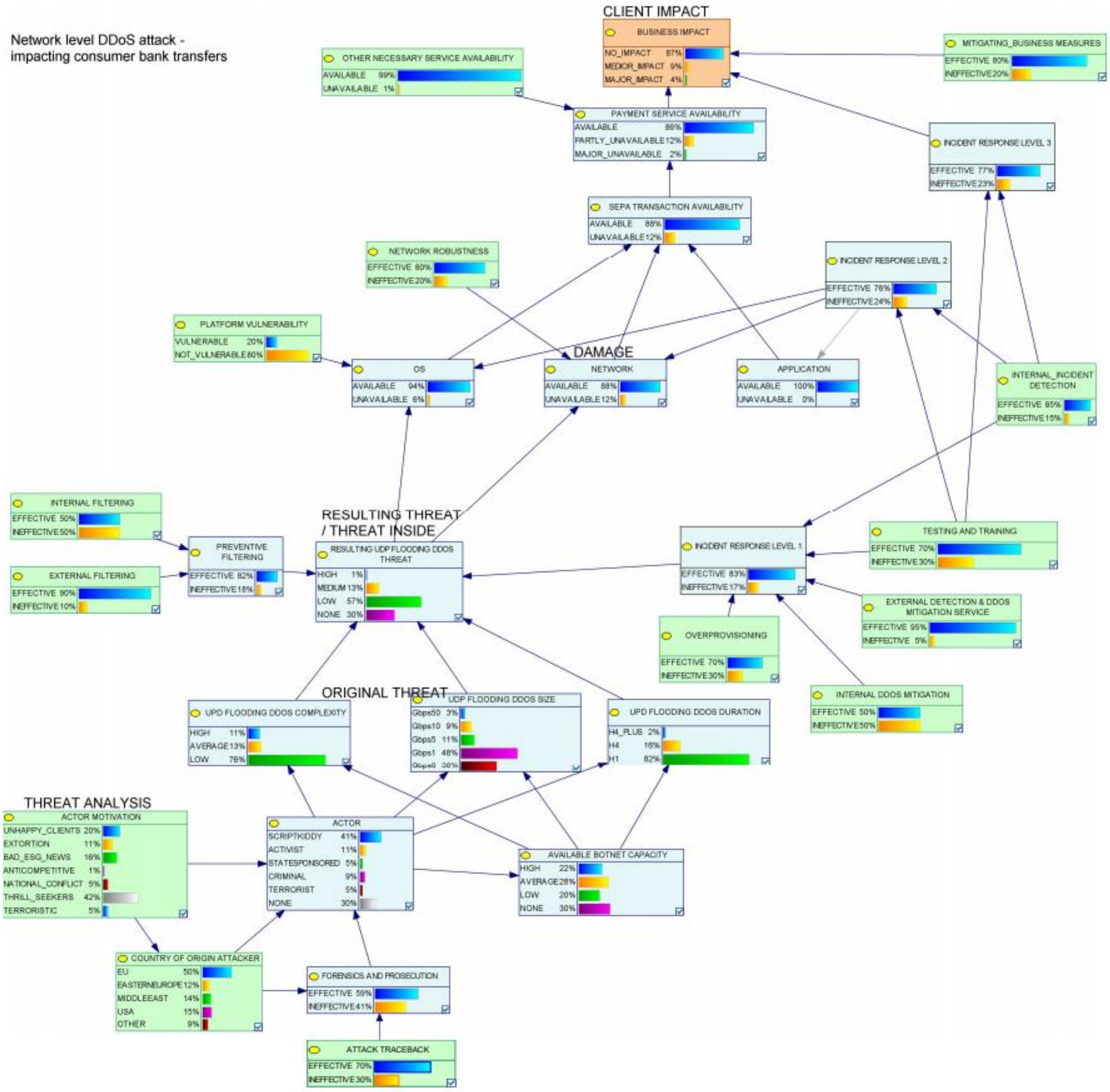
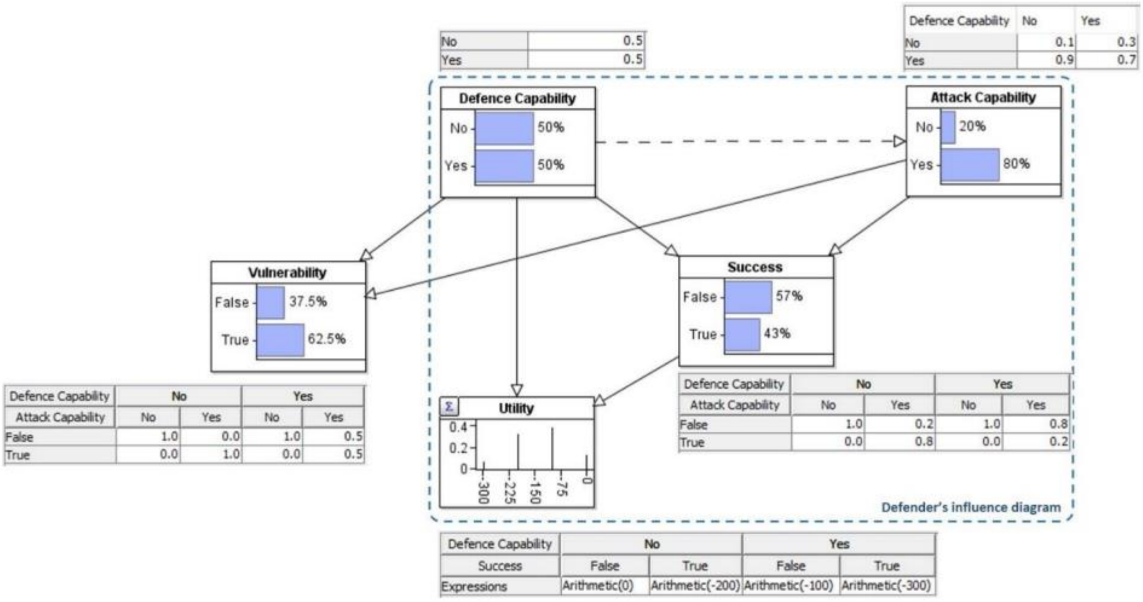


Figure 5 - Network level DDoS attack. Reprinted from (Wolthuis & Phillipson, 2019)

Wolthuis and Phillipson found that the methodology, although the development of the model took considerable effort, offers a near real-time quantitative risk assessment process. As the proof of concept was considered useful and beneficial, the authors suggest to create other use cases to test the model for its applicability for cybersecurity risks.

Other researchers have applied similar models to explore the use of decision analysis theories in cybersecurity risk assessments, like the work done by Wang on this topic (Wang et al., 2020). In his study, Wang applied a Bayesian network model to the FAIR methodology. To illustrate how such a model is visualized, figure 5 is included.



No	0.5
Yes	0.5

Defence Capability	No	Yes
No	0.1	0.3
Yes	0.9	0.7

Defence Capability	No		Yes	
Attack Capability	No	Yes	No	Yes
False	1.0	0.0	1.0	0.5
True	0.0	1.0	0.0	0.5

Defence Capability	No		Yes	
Attack Capability	No	Yes	No	Yes
False	1.0	0.2	1.0	0.8
True	0.0	0.8	0.0	0.2

Defence Capability	No		Yes	
Success	False	True	False	True
Expressions	Arithmetic(0)	Arithmetic(-200)	Arithmetic(-100)	Arithmetic(-300)

Figure 6 - Decision results - a Bayesian Network model. Reprinted from (Wang et al., 2020)

Without going into the details of the model, it is worth mentioning that models like this are suitable for capturing all relevant risk factors, their dependencies and interactions. Each individual factor is assigned a numerical probability value. Changing the value of one factor affects the values of other factors. This modeling ultimately allows for more precise predictions and decision making.

In general, it can be stated that the majority of assessments are performed using a qualitative approach. However, it is also argued that quantitative approaches would enable risk-informed decision making, opposite to qualitative approaches, enabling risk-based decision making (Pasman et al., 2017). Quantitative assessments also have the advantage of expressing results in management-specific language and enables a cost-benefit assessment. One major disadvantage of a quantitative however approach is the time-consuming process (Shameli-sendi, Aghababaei-barzegar, & Cheriet, 2016).

2.4 Comparison of risk assessment methods

In the previous paragraph we identified a number of risk assessment techniques and methods. A number of studies have been performed that compared the available methods and techniques. In this paragraph we identify the related work that has been done on this topic.

The ISO31010 standard on risk assessments includes a number of risk assessment techniques as shown in figure 2 (ISO31010 risk assessment tools and techniques). The overview includes a statement on the applicability of the technique for the three steps of risk assessment, i.e. risk identification, risk analysis, and risk evaluation. Looking at the list, it can be stated that only a few of the listed techniques and methods include all three steps of a risk assessment, i.e. those that are strongly applicable and/or applicable for all three steps. The techniques that provide in all three steps are:

- Hazard and operability studies (HAZOP)
- Environmental risk assessment
- Structure « What if? » (SWIFT)
- Scenario analysis
- Business impact analysis
- Failure mode effect analysis
- Cause and consequence analysis
- Human reliability analysis
- Reliability centred maintenance
- FN curves
- Risk indices
- Consequence/probability matrix
- Cost/benefit analysis
- Multi-criteria decision analysis (MCDA)

As we now have limited the number of potential suitable techniques and methods, they all have their own limitations and benefits which should be considered by the organization. It can for that reason be argued that specific knowledge and expertise is required to select an appropriate risk assessment technique or method.

In 2017, Agrawal compared four security risk assessment methods: CIRA, CORAS, ISRAM and IS Risk Analysis Based on Business Model (Agrawal, 2017). A comparison was made on the criteria of methodology (qualitative/quantitative), purpose of the method, input, effort required, outcomes of the method, scalability yes or no, and the respective pros and cons.

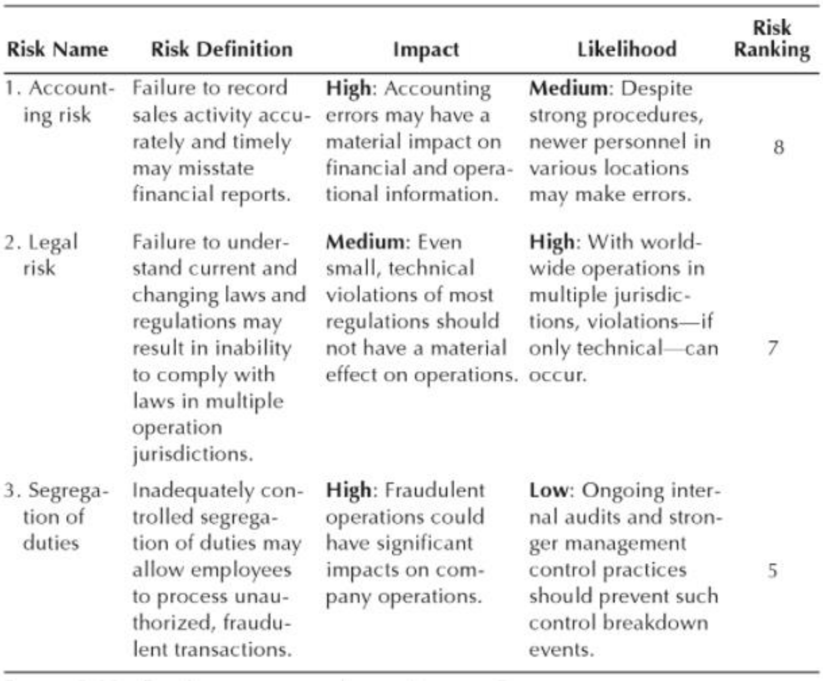
Agrawal concluded that there are many risk analysis methods are available. It is up to organizations to choose the appropriate method for their own, which can be a tiresome process, especially for small and mid-scale companies. The choice for a method heavily depends on the requirements of the organization. For example, if an organization requires numerical values on risk instead of subjective classification, ISRAM would be a potential good choice as it supports quantitative assessment.

2.5 Integration with organization-wide risk management

Organizations do not only face cybersecurity risks, there is a broad range of risks that businesses face. This paragraph explores the different types of business risks and how cybersecurity risks could be compared and integrated in an organization-wide risk profile. After all, management should be able to make a sound decision on overall business risks.

Hubbard and Seiersen argue that the different risks identified across the organization all should use the same metrics in order to get a good risk overview (Hubbard & Seiersen, 2016). Although it is likely that the different disciplines in an organization use different risk methods with respective risk ratings, in the end all those disciplines should talk the same risk language. *'If project risks are 42, cyber risks are yellow, safety risks are moderate, portfolio risks have a Sharp ratio of 1.1, and there is a 5 percent chance of new product will fail to break even, what is the total risk?*' (Hubbard & Seiersen, 2016).

In their book, Hubbard and Seiersen listed a few examples how different kinds of risk could be managed (Hubbard & Seiersen, 2016). These include Enterprise Risk Management (ERM), Governance risk and compliance (GRC), disaster recovery and business continuity planning (DR/BCP). One such example of ERM is COSO, short for Committee of Sponsoring Organizations of the Treadway Commission. COSO is a collaboration of public sector organizations and aims to provide guidance on enterprise risk management, internal control and fraud deterrence (Committee of Sponsoring Organizations of the Treadway Commission, n.d.).



Risk Name	Risk Definition	Impact	Likelihood	Risk Ranking
1. Accounting risk	Failure to record sales activity accurately and timely may misstate financial reports.	**High**: Accounting errors may have a material impact on financial and operational information.	**Medium**: Despite strong procedures, newer personnel in various locations may make errors.	8
2. Legal risk	Failure to understand current and changing laws and regulations may result in inability to comply with laws in multiple operation jurisdictions.	**Medium**: Even small, technical violations of most regulations should not have a material effect on operations.	**High**: With worldwide operations in multiple jurisdictions, violations—if only technical—can occur.	7
3. Segregation of duties	Inadequately controlled segregation of duties may allow employees to process unauthorized, fraudulent transactions.	**High**: Fraudulent operations could have significant impacts on company operations.	**Low**: Ongoing internal audits and stronger management control practices should prevent such control breakdown events.	5

Figure 7 - Integrated risk overview. Reprinted from (Moeller, 2007)

Figure 7 shows an illustrative risk list with some of the identified risks throughout the organization, and not limited to a certain discipline. Similar to other qualitative approaches, the COSO framework suggests to assign likelihood and impact values to the risks, resulting in an overall risk rating. Moeller explains that that developing such an enterprise wide risk profile is possible, given that a focused management decision process is in place. The objective of the risk assessment part in the COSO framework is ultimately to '*identify the high risk events and provide in an accurate and balanced review and assessment process.*' (Moeller, 2007).

2.6 Challenges in cybersecurity risk assessment

Academic literature describes a number of challenges when it comes to cybersecurity risk assessments. In this paragraph we elaborate on some of the main challenges with regard to risk assessments in the cyber domain.

2.6.1 Threat landscape

One of the key challenges in cybersecurity is related to the rapid changing threat landscape. New and emerging threat actors should be considered, their modus operandi, as well as the vulnerabilities those actors may be able to exploit. The 'Cyber Paradox', as referred to by Bone, challenges security and risk professionals to keep up with this ever changing threat landscape (Bone, 2016). This challenge was also raised by Henschel, arguing that attackers have the advantage of relatively easy being able to design attacks and setting the pace, while defense against those attacks requires prediction and detection techniques, acting in a reactive manner (Henshel, Cains, Hoffman, & Kelley, 2015).

2.6.2 Complexity

Another factor to consider is the complexity of cyberspace. As interconnectivity and interdependency of systems grows, the number of security risks and possible cascading effects increases. Many difficult challenges are related to the adoption of novel cyber systems (Ganin et al., 2020). The constantly changing nature of cyber systems caused by technological advances, distribution and complex network structures contributes to this complexity. In addition, specific areas of cybersecurity, like the Internet of Things (IoT), are demanding new approaches to risk assessment and management, because the regular risk frameworks do not cater for those complex environments (Kandasamy et al., 2020).

2.6.3 Lack of historic data

Other researchers identified a challenge regarding the limited data available to determine cyber risks, for example estimating the likelihood of cyber events (Garcia & Horowitz, 2015). Opposite to established domains like the insurance industry, the threats in the cyber domain change so quickly that historical data is not sufficiently available (Collier, Tehranipoor, & Lambert, 2014). The same goes for data on cyber risks, which is considered to be scarce as well (Eling & Schnell, 2016). This causes the traditional and static risk assessment methods to become obsolete (Collier et al., 2014).

As we have seen in paragraph 2.3.3, two distinctive approaches have been adopted in the risk management domain. There is the qualitative approach, expressing risks in a certain severity level. For example, risks are expressed in terms of high, medium and low. On the other hand, there is the quantitative approach, calculating risks in numbers.

Quantitative risk assessments are common practice in domains other than the cyber domain. For example, in healthcare, safety and finance quantitative risk assessment are often used (Blakley & Mcdermott, 2001). It is argued that those more mature domains have more data available to include in risk assessments compared to the relatively new cyber domain. In their paper, Blakley and Mcdermott drew an interesting comparison between the information security domain and the medical practice in the early days (Blakley & Mcdermott, 2001). As medical practitioners were considered to have a poor understanding of medical causes, symptoms or mortality rates, people had very little trust in healthcare. The public feared medication, and considered treatment to be ineffective (Blakley & Mcdermott, 2001). Nowadays, all medical treatment is being regulated and medications are thoroughly tested and measured. This is done by means of generating and collecting quantitative data (Blakley & Mcdermott, 2001). In other words, a quantitative approach to risk assessment is in place. Ideally this should also be the case for the cyber domain as a quantitative approach would contribute to the enhancement of the risk profession. As Boltz stated: "*Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing.*" (Boltz, 1999).

2.6.4 Wide variety of different cybersecurity risk assessment approaches

Organizations that want to engage in cyber risk assessments have a wide variety of tools, techniques, standards and methods to choose from.

Literature confirms that there is a wide variety of risk assessments approaches that organizations can choose from. The overview of available cybersecurity risk assessment techniques and methods as like the ones in paragraph 2.3 demonstrates that organizations can choose from a large number of approaches. This causes organizations to be in doubt what the best risk assessment approach is for their specific situation (Shameli-sendi et al., 2016).

Despite the fact that there are many approaches available to use, it is argued that at present there is no single best cyber risk model that is capable of serving all organizations (Almann & Kelly, 2008). In their paper, Almann and Kelly even question if there will ever be a one-size fits all cyber risk model.

2.7 Factors to consider when adopting a cybersecurity risk assessment approach

As we identified a wide variety of risk assessment approaches, choosing one may be a challenge for organizations. For that reason, it is necessary to be aware of the factors that should be considered when adopting one. This chapter explores literature on the relevant factors to consider when selecting a cybersecurity risk assessment approach.

The ISO31010 standard on generic risk assessment techniques states, in broad terms, that suitable techniques should meet at least three criteria. These criteria include (i) demonstrating that the approach is justifiable and appropriate to the situation, (ii) the approach should provide results in a form which enhances understanding of the nature of the risk and how it can be treated, and (iii) the approach should be capable of use in a manner that is traceable, repeatable and verifiable (International Organization for Standardization, 2019).

Furthermore, the standard provides a number of factors that should be included in the selection.

- Objective of the study
- The level of detail of assessment results needed by decision-makers
- Type and range of risks being analyzed
- ‘Riskiness’ and potential impact of the assessment scope
- Required degree of expertise, human and other resources needed
- Availability of information and data
- Need for modification/updating of the risk assessment
- Regulatory and contractual requirements

In another study, Lichtenstein identified seventeen factors to consider when choosing a security risk assessment approach (Lichtenstein, 1996). The study concluded with the importance of seven key factors: usability, credibility, complexity, completeness, adaptability, validity, and cost.

Literature review also shows studies that researched not only the available cybersecurity risk assessments techniques and methods, but also their effectiveness and/or the best fit. For example, in her Phd thesis, Labunets created an evaluation framework and theoretical model for success criteria of risk assessment techniques and methods (Labunets, 2016). Labunets studied which methods are actually effective, how methods can be validated and compared, and what criteria define the success of security risk assessment methods. The research concluded that threat-based methods are more effective over goal-based and problem-based methods. Furthermore, Labunets concluded that if a method has a clear process for the most important steps in the risk assessments, the perceived ease of use increases. A visual summary of the assessment may also contribute to the ease of use. Finally, the research also proposed future work in the area of improving existing security risk assessment methods regarding the use of tabular vs. graphical methods.

2.8 Risk assessment practices in other domains

The cyber domain is not the only domain where risk assessments are conducted. In fact, risk assessments are conducted in other domains that have been around much longer compared to the cyber domain. For that reason, it is relevant to explore how risks are assessed in other domains and how cyber risk assessments could benefit from these approaches. This paragraph explores the risk assessment practices for a couple of established domains.

A helpful analysis on this topic was done by Hubbard (Hubbard, 2020). One of the results that Hubbard analyzed in his book is a survey done by HDR and KPMG on the risk assessment methods used by respondents. The use of a risk matrix based on an international standard (like ISO, NIST), was used by 14% of the respondents. Another group used internally developed risk matrices (27%), there was a group that used other qualitative scoring or ranking methods (32%), probabilistic or math based methods was used by 20%, and 7% used methods that fit the ‘everything else’ category.

Hubbard elaborated on these categories and illustrated them with some examples of methods used in other industries. For example, the math based risk assessment methods are very common in the insurance and finance industry. Most often, these methods refer to probabilistic risk analysis, as well as quantitative risk analysis methods.

In the health industry, actual examples can be found with regard to the Covid-19 pandemic. Governments are currently managing the risks of the Corona virus on a continuous basis. For instance, the Dutch government is advised by the National Institute for Public Health and the Environment (RIVM). This institute uses (scientific) models to map the spread of the virus (National Institute for Public Health and the Environment (RIVM), n.d.). By doing so, RIVM can estimate the course of the outbreak and calculate the effect of measures. These models are quantitative by nature. Instead of using risk scales of high, medium or low, risks are expressed in numbers. There is a another parallel that can be drawn from this discipline with cybersecurity risks. Risks related to the spread of the virus and the consequences is not the only concern of the Dutch government. Other factors need to be taken into consideration as well, including social as well as economic interests. To summarize, the Dutch government needs to take into account views and inputs from different disciplines in order to make a well-informed decision on measures it wants to take.

2.9 Discussion

The results of the literature review show that risk management has emerged since the mid 1990’s (Power, 2004). The shift from an internal control focus to a risk management approach has affected the cyber domain as well. Our increased interactions with information systems and technology created a dependency in the sense that new approaches to security were required. The results of the literature review support the idea that improved ways of securing the cyber domain is necessary.

The literature review also confirms that the conceptualization of risk assessment has not changed over time. In the 1980’s, a definition was already drafted which is till date still a definition used in industry standards. In essence, risk assessment is the art of identifying what can go wrong, what the likelihood is that it will happen, and what the possible consequences are.

The results also demonstrate that studies have been performed on the challenges with regard to cybersecurity risk assessments. These challenges include the rapid change in threats, the complexity of the cyber domain and it’s interconnectivity, lack of historic data, and the many risk assessment methodologies available to choose from.

A wide range of available risk assessment and management methodologies are listed in literature. The results also show the development and rise of cybersecurity specific risk assessment methodologies. Some of the recent papers on cybersecurity risk assessments argue that a quantitative risk assessment approach, like Wolthuis (Wolthuis & Phillipson, 2019) and Hubbard (Hubbard & Seiersen, 2016), is necessary to cater for the challenges in the cyber domain. Qualitative approaches to risk assessment do no longer cater for the current cyber domain challenges. Both authors suggested a quantitative approach with regard to determining the likelihood. Wolthuis proposes to use a Bayesian Network model to process use cases.

Literature also explains the development of quantitative risk assessments. Pasman et al. described the shift from qualitative risk assessments to mandatory quantitative risk assessments in domains where disruption of systems can introduce safety risks like physical damage and human lives (Pasman et al., 2017). It is therefore argued that cybersecurity risk assessments will need more quantitative elements for those components of cyberspace where not only security, but also safety risks arise. This way, risk-informed decision making could be enabled, instead of the risk-based decision making which is the case with qualitative risk assessments.

3 Research methodology and design

This research was conducted by means of literature research as well as a qualitative approach to empirical data collection. First, a literature review was performed on the topic of cybersecurity risk assessments. Academic papers and researches have been studied and analyzed, as well as industry best-practices and international standards. The literature review served as the basis for the second step, interviews with subject matter experts. This chapter describes what research methodology was applied and how the research design was created.

3.1 Literature review

The research started with a literature review on the topic of cybersecurity risk assessments, covering the research questions one and two (RQ1 and RQ2). During this conceptualizing phase, an analysis was performed on relevant academic resources on the topics of the cyber domain, cybersecurity, risk management in general, risk assessments, cybersecurity risk assessments, and available techniques and methods how cybersecurity risk assessments can be performed. Special attention was paid to the cyber domain in relation to assessing risks. During the literature review, risk assessment practices and approaches in other domains have been explored to determine how risk assessments are performed, and if they can be useful to the cybersecurity domain. The literature review also included an analysis on what factors should be considered when organizations want to adopt a cybersecurity risk assessment methodology.

3.2 Interviews

The empirical data collection consisted of interviews, and have been conducted in order to answer the sub questions that were not part of the literature review. This qualitative approach was chosen as this especially contributed to the exploratory part of the research. The sub questions that are related to the interview part include [i] the reason why organization conduct risk assessments (RQ3), [ii] what cybersecurity risk assessment approaches organizations take (RQ4), and [iii] what limitations and benefits organizations experience in the adopted cybersecurity risk assessment approach (RQ5).

Interviews with eighteen subject matter experts in the field of cybersecurity were performed (N=18). During the interviews, participants elaborated on the choices made for certain techniques and methods, the reasons for selecting them, and potential improvement areas to cybersecurity risk assessments.

Sampling of the target population was based on the presumed knowledge and expertise of the subject matter experts with regard to security risk assessments. The interviewees were mainly from the researcher's own network. In that sense, a convenience sampling strategy was applied, where the population of the sample was close to hand (Buckingham & Saunders, 2004). In two cases, the interviewees were not part of the researcher's own network but part of the respective interviewee's network. This way of scoping the sample population is also referred to as the 'snowball effect' (Sadler, Lee, Lim, & Fullerton, 2010). This enabled the researcher to gain to subject matter experts that were otherwise out of range.

The subject matter experts work at financial institutions, and at technology, retail and security consultancy/research companies. Table 3 contains an overview of the job titles of the interviewees and sector of the organization(s) that was/were discussed during the interviews.

Coding	Job title	Sector of discussed organization
1	Information security consultant	Technology
2	Senior security consultant	Retail
3	Information technology security specialist	Semi-public
4	Senior security consultant	Aviation
5	Specialist information security & privacy	Municipality
6a	Senior cyber security consultant	Energy
6b		Municipality
7	Cyber security professional	Banking
7b		Maritime
8	Information security officer	Banking
8b		Maritime
9a	Information security officer	Semi-public sector
9b		Technology
10a	Security specialist	Utility
10b		Semi-public
11	Information security professional	Banking
12	Resilience & information security manager	Telecom
13	Security expert	Banking
14	Business advisor industrial cybersecurity	OT – general
15	Security professional	Banking
16	Chief information security officer	Retail
17a	CEO security consulting company	Health
17b		Utility
18	Researcher	Utility

Table 1 - List of interviewees

In six interviews, two example organizations were discussed based on the interviewee's previous work experience at that organization. During the eighteen interviews, a total of twenty-three organizations were discussed. Not all questions could be answered for all example organizations, either due to lack of knowledge of the interviewees, or due to time-constraints.

The interviews have been performed according to a semi-structured approach. An interview plan was created beforehand in order to ensure that the relevant questions were asked during in the interviews. The semi-structured approach allowed the interviewees to elaborate on certain topics, and enabled the interviewer to ask follow-up question.

The interviews took on average forty-five minutes and were conducted by videoconferencing. Three interviews were conducted in person. One interviewee preferred to answer the questions in the interview plan by e-mail, after which the answers were elucidated by phone. After the eighteen interviews, a certain amount of saturation was achieved. I.e. answers on the questions turned out to become repetitive and little contribution to the already collected empirical data was added. For this research, the sample of eighteen interviews proved to be sufficient.

Based on the literature review, interview questions were prepared. Table 1 contains the questions in the interview plan. In order to indicate the relevance of the question for the research, a reference is included to the respective research question (RQ). For each question, it is also indicated whether the question refers to the descriptive part of the research (D), or the explanatory part (E).

Nr	Question	RQ	D / E
	General		
1	Please indicate the industry your organization is working in	-	D
2	What is the size of your organization?	-	D
	Cybersecurity risk assessment approach		
3	What is the main reason ('why') for performing cybersecurity risk assessments?	RQ3	E
4	To what extent influences the reason for performing risk assessments the choice for a cybersecurity risk assessment approach?	RQ3	E
5	What is the scope of your cybersecurity risk assessments? *E.g. organization wide, process, applications, systems*	RQ4	D
6	Has your organization adopted one or more cybersecurity risk assessment frameworks, techniques or methods? Please explain.	RQ4	D
	Risk identification		
7	How are cybersecurity risks identified? *E.g. use of lists or catalogues, use cases, previous incidents*	RQ4	D
8	What method does your organization use for the identification of cybersecurity risks? *E.g. workshops, interviews, threat modeling, use/abuse cases*	RQ4	D
9	What components do you include in the identification phase? *E.g. assets, threats, existing controls, vulnerabilities, consequences*	RQ4	D
10	To what extent does the approach allow for including new cybersecurity risks?	RQ4	E
	Risk analysis		
11	Does the approach take a qualitative or quantitative approach in rating cybersecurity risks? Why have you chosen this approach?	RQ3	D/E
12	Does your organization assign values to likelihood, consequences, overall risk level?	RQ3	D
13	Does your organization has sufficient data to determine likelihood and impact?	RQ4	D
	Risk evaluation		
14	Do you have defined an acceptable level of risk?	RQ3	D
15	How do you prioritize the identified risks?	RQ3	D
	Rationale and justification of selected approach		
16	Why has your organization adopted this framework/technique/method?	RQ4	E
17	What is/are the main benefit(s) for the selected technique(s)/method(s) that is adding value to your organization's cybersecurity risk assessment process?	RQ5	E
18	What is/are the main disadvantage(s) for the selected technique(s)/method(s) that is adding value to your organization's cybersecurity risk assessment process?	RQ5	E
19	How are cybersecurity risks weighted and compared with other types of business risks?	RQ4	D
20	To what extent is the adopted technique appropriate to your organization?	RQ5	E

21	To what extent do the results of the adopted assessment technique provide in a form which enhances understanding of the nature of the risk and how it can be treated?	RQ5	E
22	To what extent are assessment results traceable, repeatable and verifiable?	RQ5	E
CSRA improvement areas			
23	What areas of improvements do you recognize regarding the available CSRA techniques and methods?	RQ5	E

Table 2 - Interview plan

The interview data was processed both by coding and enumeration. Interview data related to the descriptive part of the research (RQ4) was mainly processed by enumeration. This includes the enumeration of cybersecurity risk assessment methodologies and techniques used, ways to analyze risks as well as the evaluation of risks.

For interview data related to the explanatory part of the research (RQ3 and RQ5), an inductive coding approach was used as a way to analyze and process the data. Coding allows for categorization of raw and unstructured data from qualitative research (Weston et al., 2001). While processing the data, codes were developed and refined based on patterns and themes that could be identified.

4 Reasons for performing cybersecurity risk assessments

In order to understand why organizations conduct cybersecurity risk assessments, this research studied the rationale for performing security risk assessments (RQ3, interview plan question 3). This chapter contains the results on this topic.

The research data shows several different reasons for conducting cybersecurity risk assessments. The majority of the organizations are facing compliance and regulation requirements, pushing them to engage in risk assessments. Reasons for conducting risk assessments also include external audit requirements, as a result of company strategy, peer pressure. Figure 8 shows the reasons mentioned for performing security risk assessments during the interviews, grouped by sector and rationale.

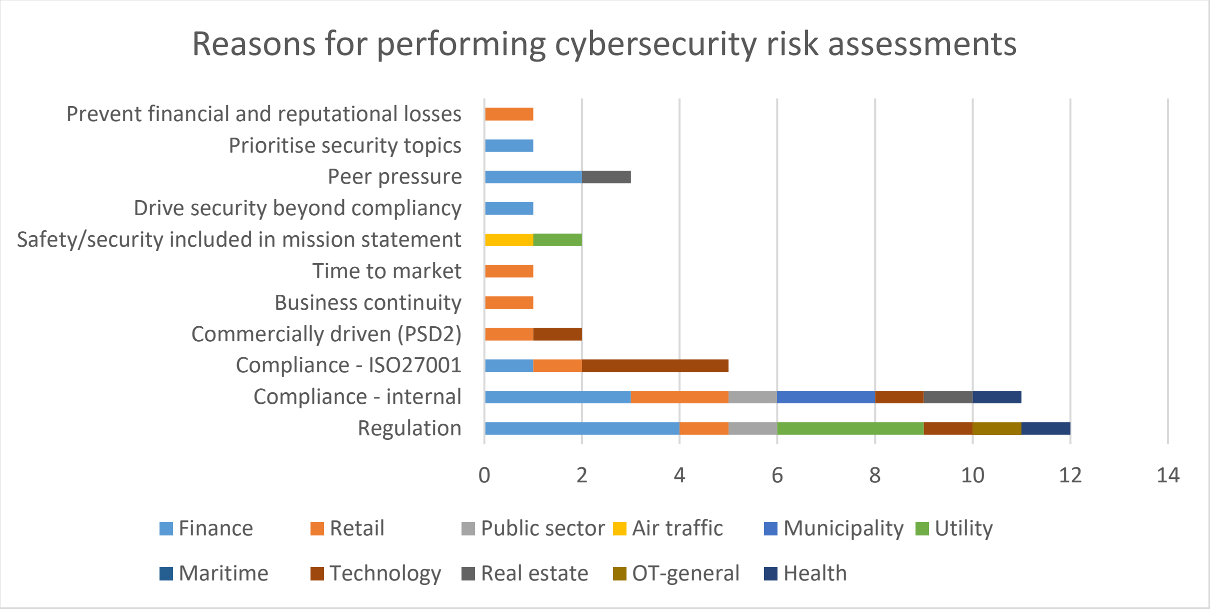


Figure 8 - Reasons for conducting risk assessments

In the following paragraphs, these reasons are explained in more detail.

4.1 Regulation

The results of this research show that the most mentioned reason for performing risk assessments is regulation. Not surprisingly, organizations operating in the energy, finance and banking, and utility industries stated that these organizations are dealing with regulatory requirements regarding risk assessments.

Financial institutions are regulated and supervised by competent authorities. Financial organizations are considered to be operators of essential services. In the Netherlands, the Dutch National Bank (De Nederlandsche Bank, DNB) supervises financial organizations. Applicable regulation is the Directive on security of network information systems (NIS Directive) (European Commission, n.d.). The Wet beveiliging netwerk- en informatiebeveiliging (Wbni) in the Netherlands is the Dutch implementation of the NIS Directive, and is legislation on cybersecurity for operators of essential services. This Directive includes topics on cybersecurity and risk management.

Not only financial organizations are subject to the NIS Directive. Another example was given by one of the interviewees working for an energy company. This organization is also regulated by means of the NIS Directive. In case the organization is hit by a cybersecurity incident, the impact can be severe in terms of human lives. From a grid management perspective, another interviewee stated that grid operators take a risk based asset management approach. This is driven by the respective supervising authority, and monitors grid operators on risk management practices, as well as expenses. This implies that expenses on for example security should be justified by an identified risk.

The General Data Protection Regulation (GDPR) was mentioned several times with regard to the protection of personal data. The GDPR is applicable for organizations processing personal data. The GDPR requires a risk assessment on the processing of personal data. This is typically done by means of a Data Protection Impact Assessment. In case the processing is likely to result in a high risk for the data subject, '*the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.'* (European Union, 2018).

4.2 Compliance

Second most stated reason for performing risk assessments is to comply with internal company policies. This means that the organization has internal policies stating that security risk assessments should be performed. Compliance may also be driven by a group entity in cases where the organization is a daughter company or subsidiary, demanding security activities in the field of risk assessments.

Results show that organizations that are dealing with cyber-physical environments, for example organizations in the energy and air traffic industry, maritime, and operational technology oriented environments, have security included in the strategy or mission statement. These organizations recognize that they do not only face security risks but especially safety and risk to human lives. This may be a strong driver for internal compliance. These research results are in line with observations made during the literature review. Similarities exist between organizations that are dealing with both security and safety concerns. Pasman identified a more mature approach to risk assessments in the industries where safety plays a role in risk management (Pasman et al., 2017). The same goes for the aforementioned organizations.

Furthermore, it was observed that organizations that have regulatory requirements with respect to risk assessments, also have internal compliance as a driver. It can be stated that regulation requirements are incorporated into internal policies in these cases.

Another rationale for performing risk assessments may also be driven by obtaining and maintaining an ISO27001 certification. Five of the discussed organizations have such certification in place. A requirement in this ISO standard includes performing risk assessments, so in order to be compliant with this standard, a risk assessment is mandatory (International Organization for Standardization, 2013).

4.3 External audit requirements

The research showed three examples of organizations that mentioned external audits to be the reason why the organization is conducting risk assessments. In one example, the external auditors required the respective organization to pay attention to cybersecurity risks. Another organization was commissioned by an external authority to conduct risk assessments.

4.4 Peer pressure

Peer pressure may also lead to the decision to perform risk assessments. In three cases, other peers drive the organization to perform security risk assessments. This drives the particular organizations to engage in the similar risk assessment practices. To cite one of the interviewees *'If others do it, we should do the same'*.

4.5 Mission statement/strategy

As explained in the paragraph on compliance, the research identified two examples of organizations stating that security and safety is included in their corporate strategy or mission statement. These organizations deliver services in the cyber-physical domain. A secure IT/OT environment is top priority for these organizations. For one of the organizations, security has become one of the four company strategies. This strategy is reflected in the organization in such a way that a risk based approach is taken throughout the organization. All business units in the organization need to consider security in their activities, in order to provide insights in risks on a business unit level.

4.6 Other reasons

Other reasons for performing cybersecurity risk assessments identified in this research include time-to-market and business continuity, to prevent financial and reputational losses and the ability to prioritize security topics. For one organization, an ISO certification was a business driver as certain countries require an ISO certification in order to do business in certain foreign countries like Japan and India. The reason for performing risk assessments in this case is commercially driven, resulting in an ISO27001 certification, which in turn makes the organization perform risk assessments.

Finally, an example was mentioned that a good security risk assessment has the ability to 'drive security beyond security', given that the risk assessments are performed by professionals.

4.7 Discussion

The results in this chapter show that the main drivers for organizations to perform risk assessments are related to regulatory and compliance requirements. Also, commercial interest and peer pressure were mentioned as drivers for performing cybersecurity risk assessments. These motivations can be considered to be rational choices for organizations; it makes sense to do risk assessments, either because they have to, or because there are incentives to do so.

Organizations operating in a cyber-physical (OT) environment have included security and safety in their mission statement and for that reason, risk assessments are part of their daily business. Only one interviewee mentioned that risk assessments were performed to drive security beyond security. It can be argued that this is an intrinsic motivation, and moving beyond the boundaries of the 'check in the box' and the mandatory activities an organization has to perform.

Results from this data demonstrate that organizations that operate in the cyber-physical domain feel the need to secure their digital domain. This is reflected in a mission statement, or in the corporate strategy. These results support the idea that those organizations recognize the possible harm to human lives in case a cyber incidents takes place. These results match with observations done in literature, like Pasman did (Pasman et al., 2017). Pasman observed that when the stakes are getting higher, like risks to safety, the need for security also increases.

5 Cybersecurity risk assessment approaches used by organizations

In order to understand how organizations conduct cybersecurity risk assessments, this research studied the approaches taken with respect to methodologies and techniques (RQ4, interview plan question 3 up to and including 15). First, the interviewees were asked for the frameworks and methodologies adopted by the organization. Next, the individual three risk assessment phases were discussed, i.e. risk identification, analysis and evaluation. In this chapter, we also make a connection between the stated reasons for performing cybersecurity risk assessments in chapter four. The adopted cybersecurity risk assessment approaches are described in more detail in the following paragraphs.

5.1 Adopted risk assessment methodologies

The interviewees were asked for the risk assessment methodology adopted by the organization. The research on the adopted risk assessment methodologies shows various approaches. In total, eighteen different approaches were mentioned by the interviewees, ranging from complete frameworks to methodologies for detailed technical risk assessments. The methodologies mentioned by the interviewees are listed in figure 9, including the sectors that the organization represents.

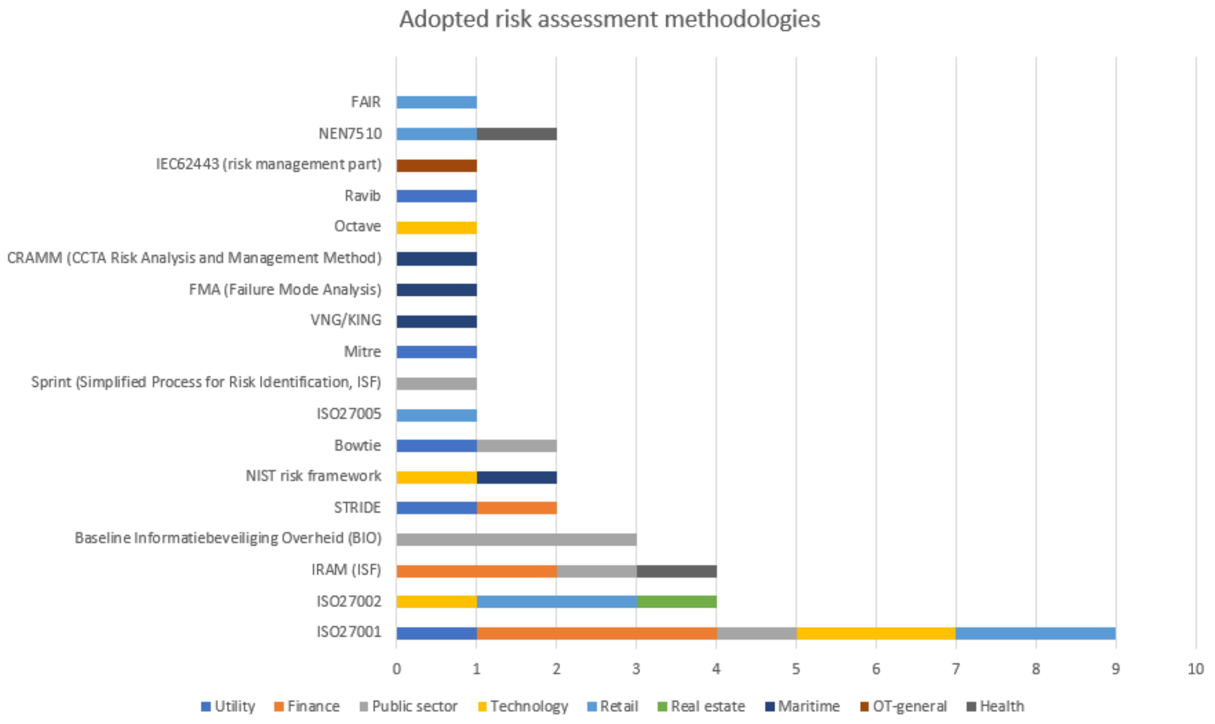


Figure 9 - Adopted risk assessment methodologies

Results from the study showed that in several cases, organizations have adopted two or more risk assessment methodologies. Table 2 contains an overview of what methodologies are used in combination and the sector the respective organization is operating in.

Methodology	Sector
ISO27002, NEN7510, FAIR	Retail
ISO27001, STRIDE, Mitre	Utility
ISO27001, IRAM, STRIDE	Finance
BIO, IRAM	Public sector
ISO27001, IRAM	Finance
ISO27001, BIO	Public sector
BIO, Ravib	Utility

Table 3 - Organizations with multiple risk assessment methodologies

The use of several methodologies demonstrates that there is a need for tailoring the risk assessment process, as well as the need for customization of risk assessment practices. The research data shows that frameworks like the ISO series on information security are used on a more organizational level, complemented with methodologies suitable for assessments on a more technical level like IRAM, STRIDE and FAIR.

Part of this research was to identify the perceived benefits and limitations of the adopted methodologies. Results on the methodologies that are most used are summarized in the next paragraphs.

5.1.1 ISO series on information security

With regard to risk assessment methodologies based on the ISO standards on information security, ISO27001, ISO27002 and ISO27005, the following benefits and limitations were identified.

Benefits of the ISO methodologies identified in this research are multiple. First of all, the ISO standard is a globally acknowledged standard that enables a reliable Information Security Management System (ISMS) including a mandatory risk assessment process. The standard includes controls that can be audited, external certification can be assessed by independent parties and the certification can be used to demonstrate security maturity and compliance. Because the ISO standard is one of the industry best practices in information security, the methodology is relatively easy to start with. The ISO standard comes with catalogues and lists that can be used to create a simple qualitative risk assessment process. A benefit in the ISO27005 standard in particular is the pragmatic approach. When adopting the full methodology, the methodology allows for an in-depth view on IT risks, including recommendations to mitigate identified risks. Also, the methodology allows for reusability of assessments.

As a downside, the methodology is considered too generic and mainly compliance driven. As this methodology uses catalogues with threats, vulnerabilities and controls as a basis, the methodology should be tailored to the organization. When the methodology is applied according to the standard, combining assets, threats and vulnerabilities, the assessment is likely to result in too many risk combinations. Results also showed that the catalogues used in the ISO series should be updated, especially with regard to threats and vulnerabilities.

5.1.2 STRIDE

The research showed that the STRIDE methodology was used in two organizations. Perceived benefits include that the methodology works well for one organization in a Continuous Integration and Continuous Development (CI/CD) environment. It was also observed that this methodology takes a proactive approach and is used for general assessments. In one other organization, STRIDE has been adopted some time now, and has become an accepted risk identification methodology.

Disadvantages of the STRIDE methodology that were mentioned during the research include the somewhat outdated methodology, as well as that at times STRIDE is difficult to use when discussing it with people from the business.

5.1.3 IRAM

The ISF IRAM methodology was adopted by four organizations. The research showed that IRAM is considered to have a good coverage of the complete risk assessment process. IRAM covers all three stages of the process, including the identification, analysis and evaluation as per the definition of ISO (International Organization for Standardization, 2018). Beneficial of the methodology is also that IRAM can spot details of threat events. I.e. the catalogue of threat events that is included is extensive and detailed.

At the same time, the detailed catalogues of threat events can cause misunderstanding when discussed with people from the business. As input from the business is required for an assessment, the IRAM risk assessment methodology is often unknown to the business. A risk assessor using the IRAM methodology should therefore be able to explain and translate the language of the methodology properly to stakeholders.

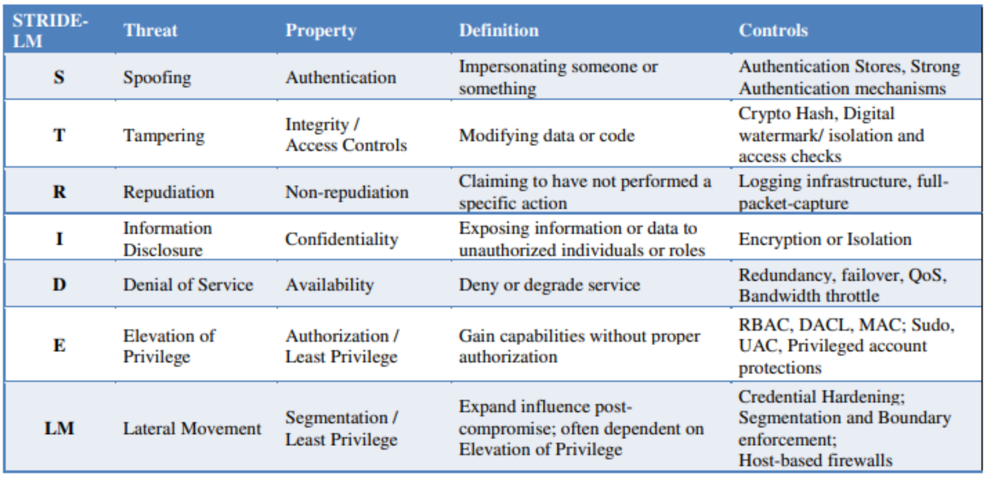
The results showed quite a number of other limitations as well. For example, the methodology requires substantial time to go through all the steps in the methodology in order to finish a risk assessment. This includes a long lead time to conduct an assessment. The methodology is therefore considered to be too full-blown.

The IRAM methodology does also not fit all types of risk assessment. The research showed an example that IRAM cannot easily be deployed for an assessment on CI/CD environments. Instead, one organization uses the STRIDE methodology for this kind of assessments.

One particular activity in the IRAM risk assessment process is performing a business impact assessment (BIA). The outcome of the BIA gives guidance on the further steps in the risk assessment. Depending on the BIA scores, the risk assessment either can stop, or it is advised to continue to the next steps in the process. During one of the interviews, an example was given that the BIA results occasionally and deliberately were downgraded in order to not have to go through the complete risk assessment process.

5.1.4 Other observations

It is noted that some of the organization were exploring a particular methodology to see whether it was a good fit. Methodologies being explored include the Baseline Informatiebeveiliging Overheid, Ravib, and FAIR. One particular methodology being investigated by an organization is STRIDE-LM. At the time of writing, the methodology was in a second stage of peer approval, and has been expanded by Lockheed Martin with the Lateral Movement (LM) aspect. The methodology was developed as an easy to access methodology and enabling risk assessors to do a proper risk assessment. Figure 10 displays an overview of the aspects covered by the methodology.



STRIDE-LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections
LM	Lateral Movement	Segmentation / Least Privilege	Expand influence post-compromise; often dependent on Elevation of Privilege	Credential Hardening; Segmentation and Boundary enforcement; Host-based firewalls

Figure 10 - STRIDE-LM by Lockheed Martin. Reprinted from (Muckin & Fitch, 2019)

Lockheed Martin, known from developing the Cyber Kill Chain, also created another methodology called the IDDIL methodology (Muckin & Fitch, 2019). A requirement for the adoption of this methodology however is that it requires experienced risk assessors to do the job.

5.2 Reason for selection

The research explored the reasons why the respective risk assessment methodology was chosen. It must be stated that not all interviewees were able to explain this reason because the methodology was already in place when they joined the organization. Nevertheless, statements could be retrieved on the reason of selection. Furthermore, the reasons mentioned for conducting cybersecurity risk assessments in chapter four allow for an analysis on the chosen methodology. This paragraph contains the results of this analysis.

In general it can be stated that the reason for the selection of a certain risk assessment methodology is driven by the context and type of organization. For organizations that hold an ISO27001 certification, the risk assessment process is prescribed by the standard. The methodology meets the minimum requirements for ISO certification. Other reasons that resulted from the research include the pragmatics that the risk assessment methodology in the ISO series on information security offers and the fit with the maturity level of the organization.

Industry best practices and globally acknowledged methodologies are considered to be another reason for selecting a methodology, referring especially to the ISO series on information security. The methodology also allows for discussions with third parties since most organizations are familiar with the ISO standards.

Another reason for selecting a methodology is driven by compliance and regulation. Organizations in the (semi) public sector are bound to frameworks for government organizations like the Baseline Informatiebeveiliging Overheid or the VNG/KING methodology. These methodologies are likely to be chosen by organizations operating in the (Dutch) government sector.

The research demonstrated that organizations are likely to adopt the ISO series on information security as a 'basic' approach to cybersecurity risks. On top of that, organizations that require a more in-depth view of particular assets are likely to adopt additional technical methodologies like SPRINT and IRAM.

The research also found that reasons for selecting a methodology may as well include recommendations from internal information security officers, or external consultants bringing a certain methodology in.

5.3 Risk identification

Risk identification is the first step in the risk assessment process. This research explored the way risks are being identified by organizations. This paragraph details the research results on this topic.

The majority of the discussed organizations, eleven cases, use catalogues as the basis for the identification of risks. These catalogues are included in the methodology that has been adopted. For example, the ISO standard on information security risk assessment includes catalogues with examples of assets, threats, and vulnerabilities that can be considered. The ISO27002 standard contains a catalogue with security controls, used in two organizations as the basis for their risk assessments. A perceived benefit of these catalogues set forth include the detection of blind spots in the risk identification phase.

However, catalogues are not the only way to identify risks. The research shows that the identification of security risks may also come from different sources. These sources include the results of penetration tests, audits, Data Protection Impact Assessments, security self-assessments, vulnerability scans and cloud intake lists. The results of these sources may be captured in a non-conformity log. In this log, all operational security issues are recorded. It is worth mentioning that the organization working with the non-conformity log has an ISO27001 certification in place. This approach was chosen because of compliance reasons, as this log is required for certification.

Another way to identify security risks is the use of 'playbooks'. These playbooks, also referred to as use cases, represent a certain security scenario. Examples of playbooks that were developed by one organization include a scenario of a ransomware attack and a scenario of a malicious insider.

This research also explored by which means risk identification is done. Results show that organizing workshops is a common practice, where representatives from the business discuss security risks together with security and risk professionals. Related to workshops are brainstorming sessions. The brainstorming sessions are perceived less directed and take a more open approach in risk identification. Other examples of risk identification and assessment in general include dedicated teams of risk assessors conducting the assessment. In these cases, the risk assessors reach out to business owners and teams in order to check the compliancy status of controls. The research results show that layered approaches to risk identification are applied at some organizations. In one case, there are two main risk instruments: a generic risk self-assessment by business owners, and a risk assessment performed by internal risk assessors. All assets need to go through the self-assessment, all asset owners are required to perform a self-assessment. Assets that are considered crown jewels are subject to a risk assessment by a security risk assessor with a frequency of every two years. Another layered approach consists of risk assessments on strategic, tactical and operational level. For each level a different methodology is used. For the strategic level, the ISO27001 standard is used, the ISO27002 standard for the tactical level, and for operational risks different sources are used that are registered in a risk register.

The scope of risk assessments for all organizations is mainly organization-wide, or on a strategic level. Results of the research shows that the majority of organizations also perform risk assessments on infrastructure and applications. Other types of risk assessments are being performed on cloud services, projects, suppliers, and in case of OT environments, Internet of Things (IoT), Industrial Internet of Things (IIoT) and Heating, Ventilation, Air Conditioning (HVAC). Other, slightly different approach have been adopted, by conducting risk assessments based on a prioritization of the most critical systems and applications in the organization. The classification of an asset is in these cases leading. Similar approaches are taken by some other organizations, where the confidentiality, integrity and availability classification levels of an asset are leading. Depending on the classification, security requirements are set.

Problem areas in the risk identification phase that were recognized include a good implementation of the risk identification. During one of the interviews, an example was given with regard to a gap in the risk identification phase. A critical system to the organization, issuing national documents, failed, and recovery was very difficult. The incident had a severe business impact on the organization and became news headlines, especially when the recovery of the system turned out to take even longer. The risk of this failing system was not identified and assessed properly.

Incorrect scoping of assessments appears to be a recipe for problematic risk identification as well. An important risk area was overlooked at one organization, that of suppliers. As suppliers often service a substantial part of IT environment, the risks associated with these suppliers were in one case not identified at all, leaving the organization with an incomplete risk overview.

Another problem area in the risk identification phase is the potential ‘explosion’ of threats when following the steps in the methodologies. It is likely that the result of the risk identification will be tens or even hundreds of possible threat scenarios, depending on the scope. In that case, grouping risks can be an alternative, however, the downside is that the risks are getting abstract or unclear.

Finally, the research results show a problem area related to conceptual and terminological confusion. Stakeholders may have different views on definitions of risks and vulnerabilities and are sometimes used interchangeable. This may hinder an efficient risk identification process. The Bowtie methodology has proven to be useful in these situations, as it helps in clarifying the risk concepts.

5.4 Risk analysis

The second step in the risk assessment process is risk analysis. This research explored how organizations perform this risk analysis activity. This paragraph details the research results on this topic.

Literature review demonstrated that risk analysis can be done in a qualitative and quantitative way. Part of the research was to explore what approach organizations take in the risk analysis phase. The majority of organizations, fourteen cases, have adopted a qualitative approach. It is argued that this qualitative approach is included in the risk assessment methodology adopted by the organization. In that sense, it can be concluded that the organization follows the risk analysis process as set forth by respective methodology.

However, the research showed two organizations taking a quantitative approach in the risk analysis phase. Remarkable is that both organizations operate in the maritime sector. The qualitative approach results from the methodology that both organizations have adopted, Failure Mode Analysis and CRAMM. Next to actually having implemented a quantitative approach, the results show a third organization exploring the FAIR methodology, which is also considered to be a quantitative approach.

During the research, several statements on the use of quantitative risk assessments were gathered. It was argued that it is ultimately up to the organization to decide how much time and effort one wants to spend on risk assessment practices, as quantitative assessments are more time consuming. It was observed that in the field of IT security it is very rare to use a quantitative approach. As an example, the comparison was made with objectifying the weather. Available data makes it relatively easy to forecast the weather. If you are dealing with hackers, this is much more difficult. However, an important benefit of quantifying risks is that it can help decide on prioritizing security topics. A business case is easier to make with a quantitative risk assessment approach.

Although most organizations do perform the risk analysis step, the research showed examples of organization that skip this phase. An alternate approach is adopted, by discussing results from the risk identification phase directly with management. The analysis of the risks is done during this discussion.

This research identified some problems areas in the risk analysis phase. First of all, a problem area is identified with regard to determining the likelihood of security risks. Determining the likelihood is often considered a difficult task, while impact determination is generally more clear. Overcoming this problem requires having a good understanding of the context of a business. A possible cause of this problem is the lack of data in the risk analysis phase. As an example, for one of the discussed organizations, nation state actors are considered to be the most serious threat. It is being questioned how to calculate the likelihood of a nation state attack and what data to use. Good data is required in order to do a proper risk analysis of such a threat. Currently, in most cases this is done by expert judgement.

Estimating the likelihood of an event appears to be a challenge in situations where people from the business are involved, for example in risk assessment workshops. People have different views on risks and risks are perceived differently.

A final problem area that this research identified is related to the definitions used for likelihood and impact scales. This problem is likely to be inherent to qualitative risk assessment approaches where scales are used. Research results show that the scales are prone to being misunderstood. Differences between medium and high values are not clear enough. This 'objectifying' of risks is considered a challenge. Too often, this results in security experts being the ones that rate the likelihood, impact and overall risks based on their professional judgement. Furthermore, it is considered to be a challenge to translate technical risks and issues into actual business risks. The normalization process that is required for the output from vulnerability scanner tooling for example can be a challenge. The results of those scanners should be evaluated in the context of the organization, but how to effectively evaluate hundreds of identified vulnerabilities?

5.5 Risk evaluation

The third and final step in the risk assessment process is risk evaluation. This research explored how organizations evaluate risks. This paragraph details the research results on this topic.

According to the ISO series on information security, risk evaluation comprises the evaluation of the risk scenarios and levels, and evaluating these to the defined acceptance criteria (International Organization for Standardization, 2018). This research analyzed the way organizations evaluates risks that have been identified. The results show that it is common for organizations to have set thresholds, or acceptance criteria, that give guidance on risk evaluation. This means that predefined thresholds are set in the case of a scaling model from 1 to 10, or values like high, medium and low that should not be exceeded. Organizations using a scaling model could have a threshold value of 5 or higher that requires the risk to be mitigated: lowering the risk by means of implementing mitigating controls. Taking a qualitative risk assessment approach, these thresholds determine what an acceptable level of risk is to the organization. A typical way to support the risk evaluation phase is visualization in the form of risk heatmaps or risk matrices.

As already briefly referred to in the risk analysis paragraph, the research also found that some organizations do not have output from the risk analysis phase, but do discuss risk identification results directly with management. Input for this discussion include results from playbook tests, or a non-conformity log with operational risks from various sources. In these discussions, the decision on risk treatment is made, i.e. if the risk should be accepted, mitigated or transferred.

The research revealed some problem areas in the risk evaluation phase and are described below.

Challenges in the risk evaluation were discussed with regard to (OT) environments. There are well-known risks in OT environments including difficulties with patching, systems that are connected to the Internet, and testing. Updating and patching OT systems is not as easy as with IT environments. As OT systems are connected to the Internet more and more, the risk and potential impact increases substantially. This impact was illustrated with the example of an attack on an oil processing organization. If an attackers is able to gain access to the systems, the attacker could be able to change the composition of the product. The challenge resides in the evaluation of these risks and subsequent risk treatment options.

The research results show that in the risk evaluation phase, an organization should consider the context for evaluating and prioritizing risks. This raises the question how results from the risk assessment process are compared to other types of risks that organizations face. After all, security risks are not the only business risks to consider, there are many other types of operational risks that an organization has to deal with. Other types of operational risk include financial, reputational, compliance and regulatory risks. This research explored if and how security risks are being incorporated in an organization-wide risk process (interview plan, question 19).

Although the majority of the interviewees were not able to answer this question, some statements could be retrieved on this topic.

Aggregation of risks to an organization-wide risk overview is perceived to be a difficult exercise. Mapping cybersecurity risks to other types of business risks, a common repository where all business risks come together, has proven to be not been very successful so far. One of the interviewees had tried multiple times to bring stakeholders from different disciplines together, in order to be able to create some sort of risk dashboard in order to be able to take integral decisions, similar to the COSO enterprise risk management model (Committee of Sponsoring Organizations of the Treadway Commission, n.d.). The initiative did not succeed in the end. One of the causes put forward is that there is was no agreed upon terminology across the disciplines. This observation matches with the prerequisite mentioned by Hubbard and Seiersen, arguing that in the end, all disciplines should talk the same language (Hubbard & Seiersen, 2016).

On the other hand, managing operational risks is a common practice for financial service providers. Financial organizations like banks have implemented the Basel framework. This framework includes an example of how business risks can be aggregated. For instance, the Basel framework includes risk categories that are used across the organization, like internal fraud, external fraud, and business disruption and system failures (Basel Committee on Banking Supervision, n.d.).

5.6 Discussion

The results of this part of the research show that organization have adopted a variety of cybersecurity risk assessment approaches. Most adopted methodologies are related to the ISO series on information security and follow the risk assessment process as explained in paragraph 2.2. It seems possible that organizations adopt this methodology as it is an industry best practice, known to peers, and relatively easy to implement. The ISO series on information security is also one of the few methodologies that give guidance on the complete risk assessment process: risk identification, analysis and evaluation. The research also showed that in many cases, this methodology was customized to the needs of the organization. The ISO methodology is considered generic and too extensive when fully applied. This would result in extensive risk registers and losing the connection with the risks that really matter. Not only the ISO methodology is being customized, the research showed that other methodologies are tailored as well. Such a methodology includes IRAM. The organizations that use IRAM have adjusted the risk assessment methodology as it is considered too full-blown. The research also showed that organizations do feel the need to adopt multiple risk assessment methodologies.

With regard to the risk analysis phase, the vast majority of organizations that were discussed take a qualitative approach. I.e. assigning high, medium, low scales, or using scales from one to five or ten to rate likelihood, impact and overall risks. Only a few organizations have adopted a quantitative risk assessment approach. A likely explanation for choosing a qualitative approach is that this approach is easier to implement and less costly (Bialas, 2006) (International Organization for Standardization, 2018), and that are no legal or regulatory requirements to conduct quantitative risk assessments (Pasman et al., 2017).

These results support the hypothesis that organizations have difficulties finding and implementing the right cybersecurity risk assessment methodology. The research results also confirm results from the literature review. Paragraph 2.3 provided an overview of the extensive available risk assessment methodologies and techniques. Finally, the results do support the statement of Almann (Almann & Kelly, 2008) that it can be questioned of there will ever be a one-size fit all risk assessment methodology.

6 Improvement areas for cybersecurity risk assessments

In chapter five we touched upon the benefits and limitations of individual risk assessment methodologies. Part of this research was to identify improvement areas for risk assessment practices in general. The feedback from on this topic was rather extensive. The results were analyzed and grouped in themes that were mentioned multiple times. The identified themes in the empirical data are described in this paragraph and grouped by governance, information asymmetry, accuracy, timing, standardization, and expertise.

6.1 Governance

The choice for a risk assessment methodology heavily relies on the organization, as well as the security maturity. Organizations should make their own decision and choice in risk assessment approach. It was stated that it is a utopia to think we can create one generic risk assessment framework. By the time we have created one, new frameworks and methodologies have popped up. Also, an organization should be careful in selecting a risk assessment framework. A requisite for the adoption of a methodology should also include the availability of tooling. After all, it does not make sense to create your own tooling, or adjust available tooling in order to fit your needs.

Another governance related issue was raised with regard to the bigger picture of the complete risk management process. Having a risk assessment process in place is a good thing, but when the follow-up of identified risks is lacking, the risk assessment process does not make sense. The research showed that monitoring and solving risks is not always happening as it should. Related to this topic is the lack of risk ownership. In case this ownership is not agreed upon and documented, the problem arises that decisions on risk treatment cannot be made.

Recognizing the need for risk assessments is often the result of incidents taking place. The problem with security and risk assessments is that it is very hard to prove that things did not happen because of the implemented measures. Security is often seen as expenses by management with limited added value. If no security incidents happen, there is no need to invest in security. This was illustrated during the research with an example. A system containing health data was replaced successfully. However, also a website was launched for managing the consent of the data subjects involved. This website was externally hosted in an insecure environment, potentially leading to the risk of reputation loss and data breaches. A short risk assessment was performed and discussed with management. The necessity was direct clear and proper actions were taken.

Finally, one example was given on a shift in responsibility with regard to security risk assessments. This shift, called responsible autonomy, implies more security responsibilities for the business. The question was raised if this is going to be the way forward in managing risks, a way in which business people are going to do risk assessments. The profession of risk assessments is not considered to have been developed in the past twenty years. It is questioned if the next five to ten years we will see changes to the way risk assessments are performed.

6.2 Information asymmetry

The research resulted in several observations with regard to information exchange and knowledge that play a role in the cooperation between stakeholders in a risk assessment. This phenomenon is referred to as information asymmetry. Kte'Pi (Kte'Pi, 2013) defines information asymmetry as '*a circumstance in which the parties involved in a situation—typically a transaction, as the term originates in economics—include one party who has more information or more accurate information than the other party or parties'*.

This research observed a lack of information between business people on the one hand, and security experts on the other hand that are driving the risk assessment.

First of all, security experts who are most often in the lead of security risk assessments and guiding the process are lacking solid knowledge of business processes. This is especially difficult when security experts from outside the organization are involved. In order to deliver a good risk assessment, this knowledge of the business context is required. It was argued that it is necessary to have enough good information from the business to automate parts of the risk assessment. Subsequently, automation is required to capture the dynamics of cyberspace.

While security professional are often lacking the business knowledge, stakeholders from the business often have limited understanding of security, the risk assessment process and terminology used. It has been argued that risk assessment methodologies should become more business oriented, as there is too much jargon used in the methodologies. The current methodologies are perceived too technical for lay people. The knowledge factor between business and security people is considered to be a serious problem.

Also, a risk assessor should have a solid understanding of the business and business risks in order to create a good cohesion between controls. A good cohesion of controls in a risk assessment implies having controls in place that take over a control that is failing.

Another information asymmetry example was given by one of the interviewees. A management representative was stakeholder in the security organization. A risk that was identified was not communicated properly to management by this representative, resulting in uninformed decision making. This example illustrates that one can have a good risk assessment and management process in place, but it is important what happens with the risk assessment results.

6.3 Accuracy

This research identified an improvement area for cybersecurity risk assessments with regard to the accuracy of assessment results.

It was observed that organizations that are using catalogues and lists for identifying risks, these catalogues are often considered to be too limited. The risks that are included in the available methodologies are too generic and require customization. Instead, organizations should interpret their own risks and include those in the risk identification phase. This way, organizations are able to include more realistic threats and vulnerabilities in their risk assessments.

Another factor to consider is the amount of data that the methodologies require. Taking the methodology in the ISO series on information security as an example, if one starts with only ten assets, it is likely that there will be a multitude of threats, vulnerabilities and controls. When too many risk factors are included in the assessment, the assessment tends to get useless. This way, accuracy gets lost and the risk assessment is losing value.

The research demonstrated the need for good data and information when performing a risk assessment. In practice this is not always the case. Especially the information that is needed in the risk identification and risk analysis phase should become more accurate.

6.4 Timing

Another improvement area was identified in this research, related to the timing in risk assessments.

Current risk assessment methodologies take time to conduct. Because of this time-consuming process, current risk assessment methodologies are being customized in order to gain efficiency in the process. The research showed the customization examples done on risk assessment methodologies like the ISO series on information security and IRAM. In essence, organizations should anticipate to faster responding adversaries. This observation matches Bone's statement on the cyber paradox, referring to the fact that security professionals face challenges in keeping up with the fast changing threat landscape (Bone, 2016). The research showed that lack of time and resources results in a shift towards a threat modeling or threat based approach. This approach may be useful for the identification of security risks, however, in general these approaches do not cater for risk analysis and risk evaluation, as well as a mapping with security controls.

Another concern with respect to timing relates to the frequency of performing risk assessments. Risk assessments should be performed more often in order to get an accurate view and understanding of the risk profile. The research showed that risk assessments are conducted as a one-off, or have a frequency of once a year at best. A one-time risk assessment is not sufficient. A risk assessment is a snapshot of current threats, vulnerabilities and control effectiveness. It is for that reason argued that we should move to a more continuous process, or at least towards a situation where real-time information can be used in the risk assessment.

An example on the frequency of risk assessments was shared in one of the interviews. A full risk assessment is conducted every two years on the most critical applications. Depending on the criticality of the system, a risk self-assessment is performed once a year, every two years or every four years. This example demonstrates that the frequency of assessments does not cater for the fast changing threat landscape. At the same time, the current risk assessment methodologies give little guidance on a continuous process in risk assessments and the expiration date of a risk assessment. Organizations are exposed to too much risk when performing risk assessments once or every two years. In this regard, the research results show an initiative by the EU-SEC organization on continuous cloud security auditing (EU Security Certification, n.d.). The EU-SEC initiative aims to solve the concerns with regard to point-in-time approaches, windows of risks where no audit is performed, and leaving cloud customers with an outdated status of the risks associated with the cloud provider. The idea of the continuous auditing concept is that cloud providers provide a daily feed with information on their compliance status, so that cloud customers have an up-to-date view on the security status and potential risk areas of their cloud provider. This status is published every day in the STAR dashboard (Cloud Security Alliance, n.d.). Although this development looks promising, a requisite to make the initiative work is that the market has to adopt these kind of initiatives.

The research also observed the need for more nuance in the methodologies with regard to the different types of risks. The current methodologies do not cater for assessing certain types of risks in a different frequency. It is argued that it makes sense to evaluate certain risks more often. For example, strategic risks could be evaluated less compared to operational risks. The same goes for non-man-made risks like the risk of flooding or fire. for When assessing risks in the same frequency, there is a high probability that the risk assessment results in the same outcomes.

6.5 Customization of methodologies

The customization of current risk assessment methodologies was identified in the research as an improvement area. No matter what methodology is used, organizations customize and tailor the chosen methodology to the needs of the specific organization. Current methodologies are non-standardized and this means for organizations that it takes a lot of effort to implement those methodologies.

There are many different methodologies available, which can be confusing for organizations. It is argued that differences between the methodologies is not clear. This results in organizations falling back on simple Excel sheets to make the risk assessment work, organize a workshop and prioritize the risks.

Also the available different frameworks and methodologies to choose from is considered to be a burden. It was observed that some of the available frameworks are considered to be very high-level, others do not cover the full risk assessment process, or do not come with risk identification catalogues like threat events. The research showed examples of organizations that created their own framework derived from the ISO27001 standard, or created an Excel based risk assessment method. Finally, a process for integration or mapping with other business risks is lacking as well in the current cybersecurity risk assessment methodologies. It was observed that the majority of organizations in this research do not have this integration in place, except for large organizations who have implemented some sort of Enterprise Risk Management framework.

6.6 Expertise

A problem area that was identified in this research has to do with the expertise required for risk assessments. Whatever framework is used, the quality of an assessment heavily relies on the assessor's expertise. As one of the interviewees stated: *‘Depending on the assessor’s expertise, you get either compliance or beyond security.’* The risk assessor’s expertise influences to what extent the goals of the assessment are achieved. It was argued by one of the interviewees that if an average assessor is handling the assessment, the end result will be a compliant asset. If an expert assessor is managing the assessment, it will start adding value.

The research also showed that organizations hire or contract security and risk professionals to either perform cybersecurity risk assessments or transfer their knowledge to the organization. Not all organizations have this expertise in house, and have made a deliberate choice to hire this expertise. Organizations that contract external specialists should however be aware of the fact that these contractors are often not familiar with the business and business risks that the organization is operating in. Consequently, a strategy like this increases the risk of information asymmetry.

6.7 Small and medium sized enterprises

As this research is focusing on organizations that conduct risk assessment activities, the selection of interviewees was based on the assumption that the organizations they represent conduct at least some risk assessment activities. The organizations that have been discussed in this research conduct risk assessments because of regulation, compliance requirements and are in general big companies or have an above average security maturity level. This leaves one category of organizations unspoken. These concern the small and medium-sized enterprises (SMEs). According to the European Commission, SMEs represent 99% of all business in the European Union (European Union, n.d.).

For SMEs, performing security risk assessments might very well be not feasible. The research data shows that SMEs do not have that many options for performing risk assessments. This matches Agrawal's observation that for small organizations, the risk assessment process and selection of an appropriate methodology can be tiresome (Agrawal, 2017). Whatever SME is involved, they are likely to process and store sensitive and/or valuable documents. Hiring external expertise will be too expensive in many cases. The same goes for implementing an Information Security Management Systems (ISMS). The research showed that the security posture of an SME is pretty vulnerable. As they are often part of the bigger supply chain, one could argue that the SMEs endanger the supply chain as a whole because they do not have the resources to conduct risk assessments. In turn, this should be taken into account by organizations that consume services of SME's.

6.8 Discussion

The results of this chapter indicate that organizations are facing problems with implementing and operating a risk assessment process. The research identified problem areas including the need to customize the current methodologies, as well as information asymmetry. This research demonstrated that the current methodologies are often considered too broad, vague or too extensive, which results in customization of the respective methodology.

The research demonstrated that information asymmetry is considered to be a major problem area. The disconnection between risk and security professionals on the one hand, and people from the business on the other hand have difficulties in understanding each other. Cybersecurity risks and the methodologies used are often not understood properly by business. These observations can be related to some of the identified challenges in cybersecurity risk assessments, including the rapid changing threat landscape (Bone, 2016), and the complexity of the cyber domain (Ganin et al., 2020). On the other hand, security and risk professionals conducting the risk assessments have problems understanding the business risks and obtaining the right information.

It is noticed that many of the identified problem areas are related to the choice of a risk assessment methodology. The research identified problem areas that match the selection criteria included in the ISO series on information security (International Organization for Standardization, 2019). Those criteria should include for example the level of detail of assessment results needed by decision-makers, the type and range of risks being analyzed, the 'riskiness' and potential impact of the assessment scope, the required degree of expertise, the availability of information and data, and the need for modification and updating of the risk assessment. For that reason, it is argued that organizations do have problems in selecting a good risk assessment methodology.

The results further support the hypothesis that current methodologies do not fit the needs for the dynamic and fast changing threat landscape. The results show that organizations predominantly use lists and catalogues that are included in the available methodologies. The results also show that these lists and catalogues are considered too generic and broad. Furthermore, it was observed that there is a need for more continuous and real-time insight in cybersecurity risks. Developments in the cybersecurity risk assessment field like the quantitative methodology proposed by Wolthuis (Wolthuis & Phillipson, 2019) look promising and could contribute to the aforementioned problem areas.

7 Conclusion

This research explored the current state of risk assessment practices in organizations. The main research question for this study was “To what extent do organizations use available cybersecurity risk assessment techniques and methods, and what is the reason for (not) selecting them?”. In this chapter, the results of the research are summarized and concluded on the basis of the formulated research questions and hypotheses.

The research questions that were drafted:

> RQ 1 - What cybersecurity risk assessment techniques and methods are there?
>
> RQ 2 – What factors should be considered when selecting a cybersecurity risk assessment approach?
>
> RQ 3 – Why do organizations perform cybersecurity risk assessments?
>
> RQ 4 - What cybersecurity risk assessment approaches do organizations take?
>
> RQ 5 – What limitations and benefits are recognized with regard to the adopted cybersecurity risk assessment approach?

In order to understand what cybersecurity risk assessment methodologies available to choose from (RQ1), literature was studied to create an overview of available methodologies and techniques. Multiple sources were identified with approaches to risk and cybersecurity risk assessments. The ISO standard on risk management (ISO31010) contains a list of generic risk assessment methodologies that can be applied. It was observed that only a few methodologies support the complete risk assessment process of identification, analysis and evaluation. For organizations, this is something to be aware of. Depending on the requirements for a risk assessment approach, organizations should select a risk assessment methodology that fits their needs.

More specific to cybersecurity risk assessments, this research concludes that there are tens of different risk assessment methodologies and techniques that organizations can choose from. Those range from full security risk management frameworks like the ISO series on information security where risk assessments are part of, to more detailed and technical risk identification techniques. The empirical data confirms that organizations take many different risk assessment approaches. Adopted risk assessment methodologies vary from organization to organization, and organizations adopt multiple risk assessment methodologies to cater for the needs. It can be concluded that organizations have many choices available to set up a cybersecurity risk assessment process.

Part of this research was the analysis of the rationale for organizations to conduct cybersecurity risk assessments (RQ3). A large majority of the organizations that were discussed in this research are bound to regulatory and compliance requirements, driving the organizations to engage in cybersecurity risk assessments. Authorities monitor organizations that are subject to regulation on conducting risk assessments. In case of compliance driven risk assessments, the driver may be organizational internal policies or an ISO27001 certification. The research demonstrated that organizations may also perform cybersecurity risk assessments because of peer pressure, driven by commercial incentives, or because management of the organization simply recognizes the need for security and safety. The latter was illustrated by organizations that have included security and safety in their mission statement or company strategy.

Part of the research was the analysis on risk assessment approaches used by organizations (RQ4). It was observed that the drivers for performing risk assessments (RQ3) influence the choices for a risk assessment methodology. The research showed that the risk assessment approaches that have been adopted do fit the needs of the organization. Organizations that are regulated adopt methodologies that are promoted by an authority, or use a methodology that is required from a compliance perspective. However, the research also demonstrated that the actual implementation of a risk assessment methodology or framework is often problematic, and that the effectiveness of the risk assessment process can be questioned. Important identified reasons for this include information asymmetry and the use of qualitative risk assessment approaches, a dominant risk assessment approach that was identified in this research. Almost all organizations use some sort of scale to rate likelihood, impact and overall risk. This may be a high, medium, low scale, or scales from one to five, sometimes plotted on a risk matrix or dashboard. As Hubbard and Seiersen argued, using scales introduces the risk of misunderstanding the definitions of these scales (Hubbard & Seiersen, 2016).

This research concludes that information asymmetry is a concern in the cybersecurity risk assessment practice and thus, an improvement area. The research showed different situations where information was lacking or misunderstood. Information asymmetry is present in the relation between security and risk practitioners, and people from the business. Risk practitioners need a sound understanding of what is going on in the business and the business risks. The other way around, people from the business do not understand the jargon and risk assessment methodologies used.

Potential improvement areas were identified in this research with regard to cybersecurity risk assessments (RQ5). The analysis of these improvements areas resulted in a grouping of improvements areas. Good governance of risk assessments and risk management is considered important in order to make the risk process work. Risk assessments should be part of a risk framework, where also care is taken of the follow-up and monitoring of risk assessment results. This is sometimes lacking. This way, putting effort in risk assessments does not make sense. Governance concerns also include the absence of risk ownership, or that organizations are too much incident driven. An incident has proven to be a good driver for gaining management commitment to risk assessments.

This research started with two hypotheses regarding cybersecurity risk assessments. The first hypothesis raised is that organizations are facing challenges in assessing their cybersecurity risks due to the wide variety of available cybersecurity risk assessment methodologies and their respective differences. Both literature review as well as the empirical data show that a broad range of risk assessment methodologies and techniques are available and used for assessing cyber risks. The empirical data demonstrates that organizations adopt risk assessment methodologies that are compliant with requirements from authorities, standards or industry best practices. Those (extensive) frameworks usually cover the complete risk assessment process, including the identification, analysis and evaluation of risks. From a compliancy perspective, these methodologies fit the needs of regulators or certification bodies. A frequently mentioned remark on the methodologies is that they are too high-level, vague and not specific to the organization. As a result, an organization adopts a methodology and customizes it to fit their own needs. The research also showed that organizations adopt additional methodologies in order to gain more detail in the identification phase on a technical level. Examples of additional adopted techniques include STRIDE, Mitre and IRAM. It is argued that industry standards like the ISO series on information security are adopted to fit the needs of regulation and compliance. From a bottom-up perspective, security and risk professionals deem to find these methodologies too high-level and have started to adopt additional techniques to spot the detailed risks. The research clearly demonstrated that current established cybersecurity risk assessment methodologies are customized to the organization.

The second hypothesis in this research is that the current methodologies do not cater for the challenges in the cyber domain with unreliable assessment outcomes and uninformed decision making as a result. This research demonstrated that information asymmetry in the risk assessment practices lead to unreliable assessment results. Risk and security professionals have difficulties understanding the actual business risks, business people do not fully understand the cybersecurity risk assessment methodologies and the terminology used in these methodologies. Organization-wide risk frameworks, where all business risks come together, are used only in the largest organizations that have some sort of Enterprise Risk Management framework in place. For most other organizations, this just does not seem feasible. A common taxonomy used for cybersecurity risk assessments would be beneficial to both risk professionals as well as business to reduce information asymmetry.

This research concludes that the developments in the cybersecurity risk assessment field in the direction of a more quantitative approach look both promising and logical. The empirical data from this research shows that qualitative risk analysis often results in problems with rating risks. This is in line with observations from Hubbard (Hubbard, 2020). Risk scales are misunderstood or not defined clearly. Quantitative risk assessments are common practice in other, established domains, like health, insurance and safety. Those domains have in common that safety is a key requirement. It is argued that the stakes are higher in these domains, or, as the ISO series on information security phrases it, the ‘riskiness’ of a cyber activity to be assessed (International Organization for Standardization, 2019). Decision makers need accurate risk analysis data in these domains to make the right and balanced choice. A quantitative approach could contribute to this requirement, as argued by Pasman (Pasman et al., 2017). Quantitative approaches also support the visualization of risk assessments. The example figures of quantitative models used in this research illustrate how visualization could be applied. As Labunets argued, a visual summary of the assessment may also contribute to the ease of use of risk assessments (Labunets, 2016).

The rapid developments in cyberspace, the increasing interconnectivity and the increase in cyber-physical applications may lead to a point where safety becomes even more important in the cyber domain compared to security of IT systems and information. As we have seen in other domains, regulation may at a certain moment in time mandate the application of quantitative risk assessment approaches as the cyber domain becomes even more critical to our daily lives (Pasman et al., 2017).

8 Evaluation and future research

The design of the research was based on a qualitative approach. By means of interviews, useful insights were collected from risk and security practitioners with regard to risk assessment in the cyber domain. The results of the empirical data confirm the problems areas already identified in literature. These include complexity of methodologies, need for customization of methodologies, and the adoption of mainly qualitative risk assessment approaches. One aspect that is not covered in literature to that extent is the information asymmetry as a concern. This research demonstrated that information asymmetry plays an important role in cybersecurity risk assessments. Future research might include ways to solve information asymmetry in the cybersecurity risk assessment practice.

The research was aimed at organizations that conduct cybersecurity risk assessments. The selection of interviewees was done based on their assumed experience with organizations that conduct these assessments. The sample of organizations discussed in the research shows that these are larger organizations and with a relative high security maturity level. Out of scope of this research are organizations that do not perform cybersecurity risk assessments. It is argued that for small and medium sized companies, performing risk assessments is often not feasible. This leaves those organizations with an unknown risk profile. The organizations that served as an example in this research are in general big companies with resources available for risk assessment practices, and in that sense do not represent the 'typical' organization. Attention should be paid to these small and medium sized enterprises to enable them to perform at least some basic risk assessment activities. It is argued that many of these small and medium sized organizations are part of the bigger supply chain. Not only does not performing cybersecurity risk assessments pose a risk to these organizations themselves, but also to the supply chain in general. It is an interesting subject for future research to investigate how these small and medium sized organizations deal with potential cybersecurity risks they are facing.

Possible future research also includes the effectiveness of quantitative risk assessment methodologies. Arguments for and against quantitative risk assessment methodologies were discussed in this research, as well as some quantitative risk assessment methodologies, like the methodology that was proposed by Wolthuis (Wolthuis & Phillipson, 2019). Future research can include building on this methodology and incorporate other uses cases, and evaluate the use of the methodology against problem areas in the current methodologies as identified in this research.

9 Annexes

9.1 List of tables

9.2 List of figures

10 References

Agrawal, V. (2017). A Comparative Study on Information Security Risk Analysis Methods. *Journal of Computers*, *12*(1), 57–67. https://doi.org/10.17706/jcp.12.1.57-67

Almann, L., & Kelly, J. J. (2008). CRS report for Congress - Economic Impact Cyber-Attacks. *Policy Review*, 39+. https://doi.org/Article

Basel Committee on Banking Supervision. (n.d.). The Basel Framework. Retrieved from https://www.bis.org/basel_framework/index.htm?m=3%7C14%7C697

Bialas, J. (2006). Security of information and services in modern institution and company. *WNT*.

Blakley, B., & Mcdermott, E. (2001). Information Security is Information Risk Management. *Proceedings of the 2001 Workshop on New Security Paradigms*, 97–104.

Boltz, J. (1999). *Informational Security Risk Assessment: Practices of Leading Organizations*. DIANE Publishing.

Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I. *Edpacs*, *54*(5), 1–11. https://doi.org/10.1080/07366981.2016.1247564

Buckingham, A., & Saunders, P. (2004). *The survey methods workbook: From design to analysis.* Polity Press.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers and Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Cloud Security Alliance. (n.d.). CSA Security Trust Assurance and Risk (STAR). Retrieved November 23, 2020, from https://cloudsecurityalliance.org/star/

Collier, Z. A., Tehranipoor, M. M., & Lambert, J. H. (2014). Cybersecurity Standards : Managing Risk and Creating Resilience, (September). https://doi.org/10.1109/MC.2013.448

Committee of Sponsoring Organizations of the Treadway Commission. (n.d.). COSO. Retrieved December 13, 2020, from https://www.coso.org/Pages/default.aspx

Cox, L. A. (2012). Confronting Deep Uncertainties in Risk Analysis. *Risk Analysis*, *32*(10), 1607–1629. https://doi.org/10.1111/j.1539-6924.2012.01792.x

De Nederlandsche Bank. (2020). *Good Practice Informatiebeveiliging 2019/2020*.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance ?, *17*(5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122

EU Security Certification. (n.d.). EU-SEC - Continious Auditing Certification. Retrieved November 21, 2020, from https://www.sec-cert.eu/eu-sec/Continuous_Auditing_Certification

European Central Bank. (n.d.). Cyber resilience. Retrieved from https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

European Commission. (n.d.). NIS Directive. Retrieved November 23, 2020, from https://ec.europa.eu/digital-single-market

European Union. (n.d.). Internal Market, Industry, Entrepreneurship and SMEs. Retrieved November 21, 2020, from https://ec.europa.eu/growth/smes/sme-definition_en

European Union. (2018). General Data Protection Regulation.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis*, *40*(1), 183–199. https://doi.org/10.1111/risa.12891

Garcia, A., & Horowitz, B. (2015). The Potential for Underinvestment in Internet Security : Implications for Regulatory Policy, (June). https://doi.org/10.1007/s11149-006-9011-y

Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, *497*(7447), 51–59. https://doi.org/10.1038/nature12047

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human Factor in Holistic Cyber Security Risk Assessment. *Procedia Manufacturing*, *3*(Ahfe), 1117–1124. https://doi.org/10.1016/j.promfg.2015.07.186

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity : An international comparison. *Computer Law & Security Review*, *29*(3), 236–245. https://doi.org/10.1016/j.clsr.2013.03.003

Hubbard, D. W. (2020). *The failure of risk management: Why it's broken and how to fix it.* John Wiley & Sons.

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk.* Wiley.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. *Sci.Int.(Lahore)*, *26*(4), 1607–1609.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information security management*. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management*.

International Organization for Standardization. (2019). *ISO IEC 31010:2019 Risk management — Risk assessment techniques*. Retrieved from https://www.iso.org/standard/72140.html

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *Eurasip Journal on Information Security*, *2020*(1). https://doi.org/10.1186/s13635-020-00111-0

Kaplan, S., & Garrick, B. J. (1980). On The Quantitative Definition of Risk, *I*(I). Retrieved from http://courses-images-archive-read-only.s3.amazonaws.com/wp-content/uploads/sites/1270/2016/12/24201241/kaplan_risk.seminal_1981.pdf

Kte'Pi, B. (2013). Information asymmetry. In *Encyclopedia of Crisis Management*. SAGE Publications.

Labunets, K. (2016). *Security Risk Assessment Methods: An evaluation framework and theoretical model of the criteria behind method's success*. University of Trento.

Lichtenstein, S. (1996). Factors in the selection of a risk assessment method, 20–25.

MITRE. (n.d.). Mitre Att&ck. Retrieved September 22, 2020, from https://attack.mitre.org/

Moeller, R. R. (2007). *COSO enterprise risk management: understanding the new integrated ERM framework.* John Wiley & Sons.

Muckin, M., & Fitch, S. C. (2019). *A Threat-Driven Approach to Cyber Security*. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

National Institute for Public Health and the Environment (RIVM). (n.d.). Modelling the spread of the novel coronavirus. Retrieved November 28, 2020, from https://www.rivm.nl/en/novel-coronavirus-covid-19/modelling

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from https://www.nist.gov/cyberframework

Pan, L., & Tomlinson, A. (2016). A systematic review of information security risk assessment, *6*(2), 270–281. https://doi.org/10.2495/SAFE-V6-N2-270-281

Pasman, H. J., Rogers, W. J., & Mannan, M. S. (2017). Risk assessment: What is it worth? Shall we just do away with it, or can it do a better job? *Safety Science*, *99*, 140–155. https://doi.org/10.1016/j.ssci.2017.01.011

Peltier, T. R. (2005). *Information security risk analysis*. CRC press.

Pescaroli, G., & Alexander, D. (2015). A definition of cascading disasters and cascading effects: Going beyond the “toppling dominos” metaphor.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. Demos.

Rot, A. (2008). IT Risk Assessment: Quantitative and Qualitative Approach.

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers and Security*, *65*(2017), 77–89. https://doi.org/10.1016/j.cose.2016.10.009

Sadler, G. R., Lee, H. C., Lim, R. S. H., & Fullerton, J. (2010). Recruitment of hard-to-reach population subgroups via adaptations of the snowball sampling strategy. *Nursing & Health Sciences, 12(3)*, 369–374.

Shameli-sendi, A., Aghababaei-barzegar, R., & Cheriet, M. (2016). Taxonomy of Information Security Risk Assessment (ISRA). *Computers & Security*, *57*, Pages 14-30. https://doi.org/https://doi.org/10.1016/j.cose.2015.11.001

Trespass Project. (2014). *Currently established risk-assessment methods*. Retrieved from http://www.trespass-project.eu/sites/default/files/Deliverables/D5_2_1.pdf

Trespass Project. (2015). *Currently established risk-assessment methods*. Retrieved from https://www.trespass-project.eu/sites/default/files/Deliverables/D5_2_1.pdf

van den Berg, J. (2017). Cyber Security for Everyone. https://doi.org/10.1145/123 4

van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boeke, S., Van Koppen, L., … De Bos, T. (2014). On (the emergence of) cyber security science and its challenges for cyber security education. *NATO STO/IST-122 Symposium in Tallin*, (c), 1–10.

Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers and Security*, *89*, 101659. https://doi.org/10.1016/j.cose.2019.101659

Weston, C., Gandell, T., Beauchamp, J., McAlpine, L., Wiseman, C., & Beauchamp, C. (2001). Analyzing interview data: The development and evolution of a coding system. *Qualitative Sociology, 24(3)*, 381–400.

Wolthuis, R., & Phillipson, F. (2019). Quantifying Cyber security Risks. *Innovating in Cyber Security: Shared Reseach*, (August), 20–26.