Inés Martínez Bustamante

DRIVERS AND IMPEDIMENTS FOR CYBER INSURANCE ADOPTION AMONG DUTCH SMEs

TU Delft

Cover image created by Sergio Árciga Bustamante.

Drivers and impediments for cyber insurance adoption among Dutch SMEs

by

Inés Martínez Bustamante

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE
in **Complex Systems Engineering & Management**

Faculty of Technology, Policy and Management
Technische Universiteit Delft
Delft, Netherlands

To be defended publicly on Monday August 27^{th}, 2018 at 15:00

Graduation committee

Chairman	Prof.dr. M.J.G. van Eeten	POLG
First Supervisor	Dr.ir. W. Pieters	SE & S
Second Supervisor	Dr. M.L.C. de Bruijne	POLG
External Supervisor	Dr. K. Labunets	SE & S

This thesis is confidential and cannot be made public until August 27, 2018.

An electronic version of this thesis is available at `http://repository.tudelft.nl/`.

TU Delft Delft University of Technology

Acknowledgments

If someone is keeping count of how hard an MSc. thesis is, please add a +1 to that count.

During the last months, there have been complicated days related to the work for this thesis. To escape from the daily routine, before going to bed I would usually try to read a couple of pages of whatever book I had at the time. One of these nights, a phrase hit me, "Certainty is the enemy of growth". I thought I was certain about the implications of doing a Master program, I am glad I was wrong. The pleasure of achieving the personal goal of moving abroad and completing an MSc. in this great university is indescribable. However, this pleasure is nothing if it is not shared, it is thanks to my network of people I established here.

First and foremost, I want to thank my external supervisor, Kate Labunets. We started to talk about the project back in November 2017, when I was still in Japan. Since that moment, she never stopped providing me with valuable feedback, references, and recommendations. Her critical comments always pushed me to look for ways to excel in my work. I really hope it was not such a burden to supervise me. Then, I would like to thank the rest of my committee for accepting to provide guidance for this research. To the Chairman, Michel van Eeten, for having a place in his busy agenda and providing me feedback when needed. My first supervisor Wolter Pieters, whose knowledge in this topic helped me in boosting my learning curve. Mark de Bruijne, my second supervisor, for his patience, advice, and willingness to read and correct the report. Next, I want to thank my interviewees, I highly appreciate your willingness to participate in this research. I learned from your experience, and I hope you will also learn something from this report. Without you, this research would not exist.

Now comes the time to thank my social circle, my friends. There are those who helped me with the proofreading and spell checking of this thesis. There are others that cheered me all the time. There are more that gave me unforgettable memories, and there are the most that have helped me to improve my vision of the world. Thanks to each and every one of you.

Most importantly, I would like to thank my family, without you I am nothing.

Inés Martínez Bustamante
Delft, August 2018

Executive summary

Introduction

The strong dependence between businesses and digital technologies is emphasized by the growing rate of cyber incidents. This dependence comes with digital security and privacy protection risks. Measures like security awareness, intrusion detection systems, safeguard infrastructure, among others, may limit the spread of cyber attacks. However, these measures have proven to not be enough since a new virus or a smarter attacker would be able to surpass all type of security measures. Because the elimination of all risks is impractical and impossible, it is necessary to implement the most appropriate controls to mitigate risks.

Here is where the insurance industry comes into play as a risk transfer strategy, with cyber insurance as a measure to complement established security controls and to help to manage the risks that cannot be fully mitigated. Cyber insurance is also contributing to manage cyber risks by raising awareness, supervising incident management and encouraging investment in security systems. While the promise of cyber insurance is high, adoption rates have fallen short of expectations. This research tries to find out why the cyber insurance adoption has not been as high as expected, focusing on the Netherlands and specifically in SMEs.

If parallel lines are drawn between acquiring cyber insurance and getting any other type of insurance, previous research has shown that under risk conditions humans do not behave rationally. Then, if this is also true for cyber insurance adoption, an approach other than developing mathematical models should be used to understand it. One way to look at this problem is by analyzing the way individuals make decisions when purchasing a product, like insurance. Behavioral theories such as the Protection Motivation Theory (PMT) can explain these decisions.

This research followed a qualitative approach based on literature review and empirical data collection supported by semi-grounded theory techniques. A series of semi-structured interviews with SMEs representatives were held to discover the decision-making process for adopting cyber insurance that exists in the companies. PMT is used as an underlying theory to build the interview questionnaire. Afterward, to analyze collected data and build the theoretical model of drivers and impediments for cyber insurance adoption, techniques from semi-grounded theory are used. The main research question to be answered is:

What decision-making process do SMEs follow to acquire cyber insurance?

Theoretical foundation

Cyber insurance has existed for more than two decades and a process to acquire it could be developed already. Nevertheless, the existing literature is based on large companies, but SMEs do not need as long as a business process as large companies do. Then, existing business processes are not enough to explain the decision-making process for cyber insurance adoption, but they are necessary to assist decision makers.

PMT is developed along two processes based on the cognitive process people follow to evaluate threats (the threat-appraisal component), and select the alternatives to handle this threat (the coping-appraisal component). As the name suggests, PMT looks into the reasons that guide people to protect themselves. The elements that form TPM in the cyber insurance context are described in Table 1.

Insurance consumer behavior can explain the process to acquire traditional insurance, where both rational and irrational behaviors are addressed. From this research, three main processes are identified to occur when a company is analyzing the acquisition of cyber insurance: the cognitive process, the emotional process, and the business process. Through PMT, the cognitive and emotional processes can be identified.

Results

Regarding the **intrapersonal** element, seven companies heard about cyber insurance for the first time through the broker, and only 2 out of 11 companies know other companies with cyber insurance. In

Sources of information	
Intrapersonal	Personality aspects and feedback from prior experience
Environmental	Verbal persuasion and observational learning
Threat appraisal	
Vulnerability	Determine the probability of experiencing a cyber attack
Severity	The extent to which the threat is severe
Rewards	Identify the reasons for not having cyber insurance
Coping appraisal	
Response efficacy	The perception to cope with the cyber attacks
Self'-efficacy	The belief that the company is able to implement a protective response
Response costs	Identify any type of costs as a consequence of adopting cyber insurance

Table 1: PMT elements in cyber insurance context

both cases, their professional network provided this approach. For the **environmental** element, only 1 of the 2 companies decided to discuss cyber insurance with another company. Finally, 5 companies knew other companies had been attacked before getting the cyber insurance, 4 of them is because of their professional activities.

Corresponding to PMT's threat appraisal component, the **vulnerability** element identified that digitalization is the main source of threat, but they also recognize digitalization as necessary for their company to grow. This is also applicable to other vulnerability factors like client's confidential information and reputation since these are aspects necessary to carry out their business. In line with the previous PMT element, comes **severity**, where the main identified security threats are phishing and leak of data. Finally, for the **rewards** element, the two main reasons companies mention not to acquire cyber insurance are price and that they perceive is not necessary.

Regarding the coping appraisal element **response efficacy**, none of the companies were asked to implement additional security controls to provide cyber insurance. For the expectations about cyber insurance, companies expect to get the appropriate help during the process in case of an attack. They also just hope not have to use the insurance. The next element, **self-efficacy**, was assessed to recognize if companies feel capable of carrying out the use of the cyber insurance, 100% of the answers indicated that the cyber insurance policy is understandable and clear. For companies that decided not to have cyber insurance, they consider having a good IT security management strategy. The last element, **response cost** is naturally related to the premium price. Most of the interviewees indicated that the price is considered to be fair.

Conclusion

Results for the business process validated that the broker is in most cases the first one approaching the SMEs to discuss the cyber insurance product. The decision-making process does not take too long due to the low number of persons involved. Moreover, an internal process was identified, which can be influenced by the level of knowledge of the personnel about IT and security.

The questionnaire helped to identify the main drivers and impediments companies have to get or not to get cyber insurance. The most common drivers are to protect the reputation, have it as a preventive measure, compensate the limited responsive status a small company has, and increase awareness. The most common impediments are a high premium price, unclear policy, and having enough protective measures.

In the end, everything comes down to understanding the process and the elements involved for SMEs to decide whether or not cyber insurance is worth having. The model shown in Figure 1 is the final result of this research. Theory showed at the beginning that the decision of getting cyber insurance could not only be guided by rational thinking like a business process. Then, PMT appeared to be able to explain the missing irrational aspect not present in the business process, but only applying PMT in the decision-making process of a company leaves out the policies and procedures existing in any company. The outcome of the theory research is to identify the three processes present during a decision-making process for insurance, which are the emotional, cognitive and business processes.

The structure of the model is as follows. For sources of information component, it can have an active or a passive role. For the threat appraisal component, there is an element that can be decisive, the state of the security protective measures. Then, the company will analyze the probability of the

attack occurring. For the coping appraisal component, the company analyzes the policy coverage. In this process, there is also an element that can be decisive, the premium price. Regarding the business process for SMEs, it does not involve too many people like in large companies, and the outcome depends on the SMEs decision-maker priorities for the company and the company guidelines. Figure 1 shows the decision-making model.

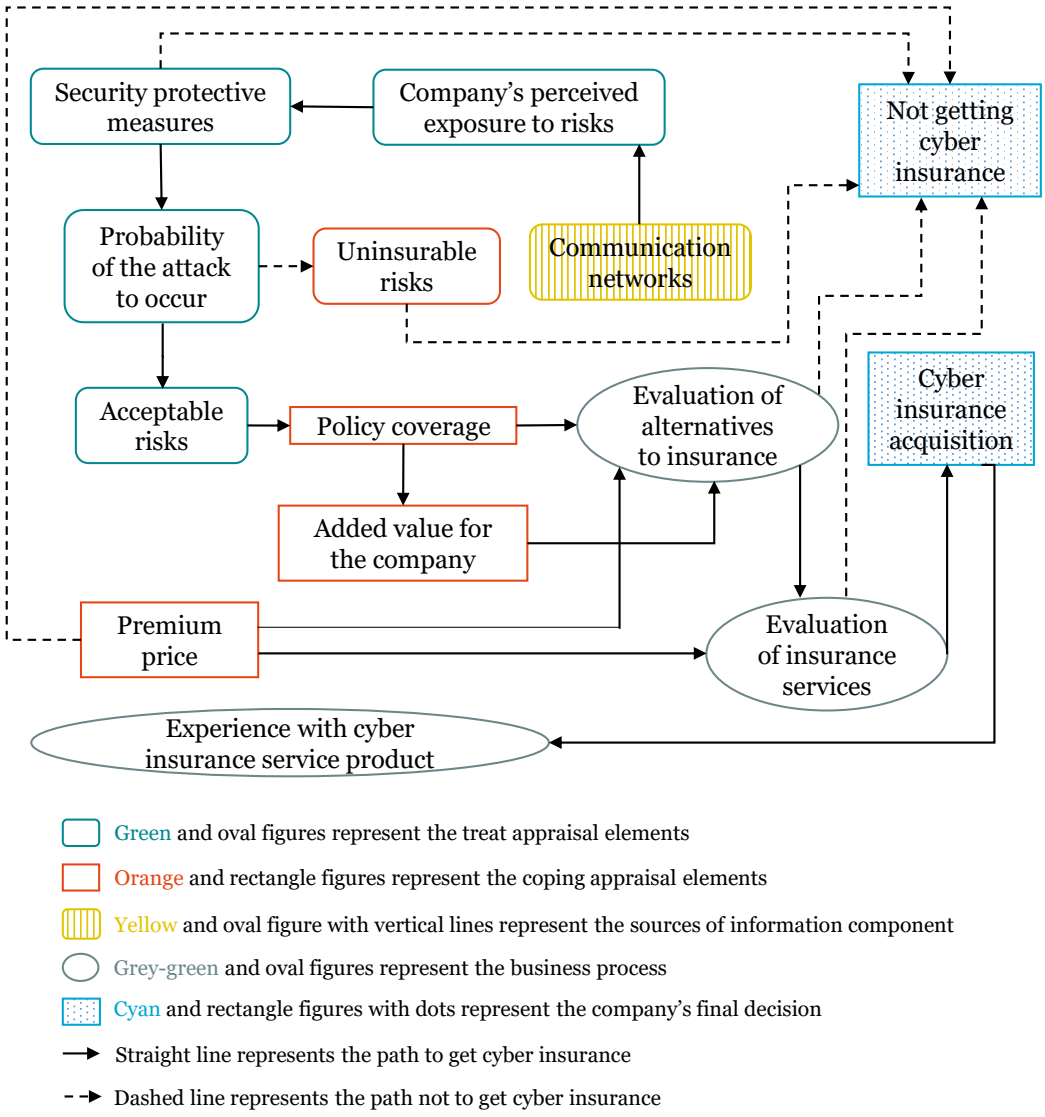


Figure 1: Decision-making model for cyber insurance adoption

Contents

List of Abbreviations

AP	Autoriteit Persoonsgegevens (Dutch Data Protection Authority in English)
CI	Cyber Insurance
CoSEM	Comples Systems Engineering and Management
EU	European Union
GDPR	General Data Protection Regulation
IT	Information Technology
PII	Personally Identifiable Information
PMT	Protection Motivation Theory
SMEs	Small and Medium Enterprises
U.S.	United States

Reading guide

Dear reader,

While reading this thesis there are certain concepts I would like you to keep in mind to avoid misunderstandings.

PMT components

Whenever you see the word component, it refers to one of the following components:

- Sources of information
- Threat appraisal
- Coping appraisal

PMT elements

Whenever you see the word element, it can refer to one of the following elements:

- Intrapersonal sources of information
- Environmental sources of information
- Vulnerability
- Severity
- Rewards
- Response efficacy
- Self-efficacy
- Response cost

See an exception at the end of this section.

Process

The word process refers to the series of actions or steps to achieve an objective. You will commonly find the concepts such as ”business process” and ”decision-making process”, among others. For instance, you will find the business process for cyber insurance adoption, which means the series of steps taken to get cyber insurance.

Model

The word model refers to the static representation of a process. Then, concepts such as ”decision-making model” and ”mathematical model”, among others, will be found throughout the report. For instance, the decision-making model is the two-dimensional representation of a decision-making process.

Element

As it was previously mentioned, the word element could refer to one of PMT elements, but it is also used to refer to a part of a model. For instance, when discussing a decision-making model you will find the description of the elements that form the model.

I hope this simple explanation make your reading lighter than without it.

List of Figures

List of Tables

1

Introduction

Chapter 1 discusses the reasoning behind the research and the structure of the report. Section 1.1 explains the growing tendency of cyber attacks with a brief introduction of cyber insurance and SMEs. Then, Section 1.2 explains the problems related to cyber insurance adoption, which leads the reader to the main research gaps founded by the researcher. In Section 1.3, the main research question and its correspondent sub-research questions are presented. Section 1.4 explains how the research questions will be answered. Next, Section 1.5 highlights the main contributions in the scientific and societal fields. Finally, Section 1.6 provides the reader with the outline of the thesis and the chapter division.

1.1. Research background

Recently, major consumer data breaches occurred with enormous impacts for companies. In late 2013, Target, a large department store in the U.S., was victim of a data breach that costed the company around $450 million. Credit and debit card's data of of 40 million customers' and personally identifiable information (PII) of 70 million customers' were compromised (Fisher, 2014). In 2014, other big store retailers like eBay, Home Depot, and K-mart also became victims of cyber criminals' through intrusion into their systems. These kinds of activities affect any business relying on digital technologies, as has been the case of the banking industry when in 2014 J.P. Morgan Chase & Company suffered an intrusion compromising the data of 7 million small business and 76 million households (Fox, 2016). It is also worth to mention one of the largest breaches in history occurred in September 2017 to Equifax, one of the world's three largest consumer credit bureaus, where the sensitive data of 145.5 million U.S. citizens were stolen, along with users' data from Canada and the United Kingdom (Hackett, 2017).

These and more recent incidents (130 security breaches on average per year worldwide, (Ponemon Institute, 2017)) emphasize that the strong dependence between businesses and digital technologies comes with digital security and privacy protection risks. Moreover, the cost of cyber crime varies per type of organization. The Ponemon Institute (2017) has found differences depending on the organizations' size, industry sector, and even country. Regarding organization's size, the bigger the company, the larger their costs and losses; for the industry sector, the financial sector has been the most affected; and regarding the country, the United States has the higher costs. Since certain types of companies are more commonly affected than others, it is not a surprise to find that news coverage, and academic research are focused on the attacks on big companies and significant investments in cyber security protection are located in the United States. Finding the existing difference in the academic research raised questions about the state of coverage for the least representative parties like small companies and countries that have not seen many attacks.

Regardless of the niche to study, protective measures like security awareness, intrusion detection systems, safeguard infrastructure, among others, may limit the spread of cyber attacks but have proven to not be enough since a new virus or a smarter attacker would be able to surpass all type of security measures. The definition of risk, according to Jones (2005), is summarized as "the probable frequency and probable magnitude of future loss". With this in mind, it has to be acknowledged that the elimination

of all risks is impractical and impossible, then it is necessary to implement the most appropriate controls to mitigate risks.

There are five main types of risk mitigation strategies: 1) accept, 2) avoid, 3) mitigate, 4) share, and 5) transfer. Complex decision processes in a company are usually preceded by the type of strategy that is selected and the appropriate risk management tools chosen. Here is where the insurance industry comes into play as a risk transfer strategy, with cyber insurance as a measure to complement established security controls and help to manage the risks that are not possible to be fully mitigated, or the treatment is too expensive while the risk likelihood is very low.

Cyber insurance has come as a complementary answer to deal with cyber risk, which was identified by the OECD as a type of risk of highest concern to doing business (OECD, 2017). Besides transferring the financial exposure, cyber insurance is also contributing to the cyber risk management by raising awareness, supervising incident management and encouraging investment in security systems (OECD, 2017). While the promise of cyber insurance is high, adoption rates have fallen short of expectations.

The economic growth of any country is closely linked with to the growth of its Small and Medium Enterprises (SMEs) (Pandya, 2012). In the Netherlands, SMEs count for about 65% of employment, with wholesale and retail industries being the biggest sectors. Moreover, SMEs represent 99.8% of all enterprises, contributing to almost 64% of the GDP, whereas the average contribution to GDP in high-income countries is around 50%. Conscious of the importance SMEs have on society, Capgemini together with the insurance company Interpolis performed cyber security scans, finding that SMEs' digital security is at an immature level (Capgemini, 2017). Meanwhile, the research group at The Hague University of Applied Sciences indicated that 20% of SMEs have been victim of cyber crime but that SMEs' diversity makes challenging to suggest one approach to deal with security threats and recommends a societal approach (Loohuis, 2018). This research tries to find out why the cyber insurance adoption has not been as high as expected, focusing on the Netherlands and specifically in SMEs.

1.2. Research problem

Cyber insurance market has existed for at least 20 years, but the literature shows that the study of this field is still developing, the U.S being the most developed market having 90% of the global cyber insurance market according to numbers in 2015 (PwC, 2015). Still, the number only counts for one third of U.S. companies. In terms of premium price, in 2011 the premium policy volume in the U.S. was around $400 - $500 million and has the projection of growing to $20 billion by 2020 (Hemenway, 2015). In terms of the value of the market, worldwide information security market was reported to be worth $75.4 billion in 2015 and projected to grow to $170 billion by 2020 (Morgan, 2015). From the U.S. experience, it can also be taught that a big company is more susceptible to getting cyber insurance than a smaller company due to factors like "still developing regulatory environment at the federal and state levels, a general lack of awareness of cyber-related business continuity risks, and an overestimation of corporate cyber security capabilities" (Bradford, 2015). For instance, 26% of the companies with a revenue of at least $5 billion have a cyber insurance, while companies with revenue lower than $500 thousand counts for 3% (Woods, Agrafiotis, Nurse, & Creese, 2017).

A common issue among insurances is the constant presence of asymmetric information from both consumer and user side. Economists like Akerlof (Akerlof, 1970) have established that trust is an important condition to execute trade and production deals and therefore, uncertainties in the insurance business due to problems like adverse selection and moral hazard could result in a low adoption of insurances. Adverse selection arises when one of the parts has more information than the other and with this they decide to participate in a trade, achieving a greater benefit. Moral hazard occurs when the insured takes more risks than it would if the purchase of the insurance had not occurred, then transferring more risks towards the insurance (Tumay, 2009).

Bandyopadhyay (2011) has summarized three reasons for which the cyber insurance market has not had a significant penetration as expected. First, correlation of cyber risk among organizations, meaning that computer systems have similarities that can be replicated affecting all type of organizations. If software is infected, the impact will be the same in the software versions across the world. Second, information asymmetry in contract design, leading to overpricing cyber insurance contracts and. Third, difficulty in evaluation of cyber loss together with insufficiency of actuarial data. These three reasons present challenges for both customers and providers since no single side is in charge of controlling

them.

Looking deeper into the market to find further explanation about the failures of cyber insurance, Franke (2017) interviewed insurance companies in Sweden, finding that differences in the offered coverage causes a lack of clarity resulting in lower adoption, and pricing model is based more on rules of thumb than on historical data and individual risk profiles of the customers. Meland (2017) interviewed Norwegian companies, finding that cyber insurance products are still perceived as immature (the market is premature and policies are not detailed enough on what they offer), and not prepared at a technical knowledge level, but it is also found that companies do not have proper cyber risk assessment prior to considering whether to get cyber insurance. Romanosky (2017) analyzed 180 policies in the U.S. to provide a clear look to the underwriting process and how insurers price cyber risks. This last point is significant since some researchers have shown that underwriting process[1] and in general the application process to get a cyber insurance can be wearisome (e.g., (Franke, 2017; Woods et al., 2017)) because it is perceived as long and complicated.

The market for cyber insurance is related to the increase in cyber incidents and together with this, privacy breach notification policies. Recently, the General Data Protection Regulation (GDPR, a regulation on data protection in European Union) is making clearer that privacy breaches can affect anyone, and because of this, companies need to take responsibility for protecting users' data. A survey estimated that after a breach, 29% of existing customers would discontinue the relationship with a company (Huth, 2018), showing the strong impact a cyber risk can have. Related with the entrance of GDPR, a higher interest in cyber insurance started to appear, according to a representative of AIG[2](AIG, 2017) since the regulation has increased the awareness level against cyber risks, including SMEs.

If parallel lines are drawn between acquiring a cyber insurance and getting any other type of insurance, utility theory has been used to analyze the process to select an insurance (e.g., (Kunreuther & Pauly, 2018; Song, Peña-Mora, & Arboleda, 2010)), showing that under risk conditions humans do not behave rationally. Nevertheless, the way in which cyber insurance adoption has been studied is through mathematical models, specifically game theory. (Hayel & Zhu, 2015) models the interaction between users, insurance companies and attackers to design insurance policies; (Tosh et al., 2017) models the same actors to study their possible decision strategies, and; (Yang & Lui, 2014) analyzes the impact of network externalities to take security adoption decisions. If cyber insurance adoption is not following a rational behavior as mathematical models suggest, a different approach should be used to understand it. One way to look at this is by analyzing the way individuals make decisions when purchasing insurance. Protection Motivation Theory (PMT) is a behavioral theory that identifies the elements guiding an individual to protect against a threat. Then, PMT is an option to explain the reasons for companies to select protection against cyber risks.

1.2.1. Research gap

As can be noticed from the previous sections, there is a research gap in the next themes:

- SMEs have been out of the scope of research on the adoption of cyber insurance since they account for a tiny part of the current cyber insurance market (as low as 2% of the market[3]). Nevertheless, research in this sector is essential as Srinidhi (Srinidhi, Yan, & Tayi, 2015) indicates that smaller companies with large insurance coverage could cause the acceleration of their capital accumulation. More important is the direct impact SMEs produce in societal and economic aspects (65% of employment and 64% GDP contribution), then, a focus in SMEs should not be left behind.

- There is a lack of information about the reasons why companies select cyber insurance due to the novelty of the cyber insurance field. Empirical research can help to fill this gap by providing insights into the way companies decide to transfer cyber risk. Also, this type of research can help to understand the way cyber insurance is adopted, along with the problems the process implies.

- If cyber insurance is meant to be considered as an incentive for improving security as suggested by the OECD (2017), the moral hazard issue has to be managed since companies can control

[1]The process to guarantee an average proportion of risks for the insurer and the insured. This process leads to determine the premium price.

[2]The American International Group, a multinational finance and insurance corporation.

[3]Numbers can vary per country according to (OECD, 2017). This number should not be confused with the one provided by Woods (2017) in Section 1.2

this behavior. To accomplish the previous, research in the demand side should be carried on. Nevertheless, this has not been the case since access to these actors is not as accessible as it is for suppliers (brokers and insurers).

- Cyber insurance adoption has been mainly studied through mathematical models but not from a behavioral point of view, to understand the reasons that lead a company to acquire or not this type of insurance.

1.3. Main research question and sub-questions

This research follows a qualitative approach based on a literature review and empirical data collection supported by semi-grounded theory techniques. A series of semi-structured interviews with SMEs representatives were held to discover their decision-making process for adopting cyber insurance. PMT is used as an underlying theory to build the interview questionnaire. Afterward, to analyze collected data and build the theoretical model of drivers and impediments for cyber insurance adoption, techniques from semi-grounded theory are used, such as coding of interview transcripts and code classification (Stol, Ralph, & Fitzgerald, 2016). The main research question to be answered is the following:

What decision-making process do SMEs follow to acquire cyber insurance?

To answer the main research question is necessary to narrow down the topic, which will be done through the next sub-questions (SQ):

1st sub-question

SQ1: How does PMT explain a companies' need for cyber insurance?

PMT is a behavioral theory that differentiates between emotional and cognitive responses, two processes initiated by a perceived fear. Cyber insurance adoption has not been studied from a behavioral perspective, so first, a proof that a behavioral theory like PMT can be applied for this purpose is provided. The purpose of this sub-research question is to describe PMT elements and translate them into the cyber insurance context.

2nd sub-question

SQ2: How can PMT be implemented in a decision-making model describing companies adoption of cyber insurance?

To know if PMT is a sufficient theory to describe cyber insurance adoption, research into existing decision-making models for insurance adoption is done. The purpose of this is two fold: first, to delineate the traditional business process to get cyber insurance, and second, to have an outline for the decision-making process. The differentiation between the business process and the decision-making process is that the first is a series of logical steps that implies a rational behavior from the actors involved, the latter is a process executed in a real-world situation, where rationality might not always apply. Since two different processes are explained, the sub-research question divides into the next sub-questions:

- What is the business process for selecting cyber insurance?
- What other factors should be taken into account to define a decision-making model?

3rd sub-question

SQ3: How does threat appraisal influences cyber insurance adoption and the decision-making process?

Threat appraisal is the PMT component explaining the way an individual perceives danger. Therefore, it can reveal the reasons for taking protective measures against cyber risks. The objective is to explain the type of influence the threat appraisal elements have and the role the component has during the decision-making process.

4th sub-question

SQ4: How does coping appraisal influences cyber insurance adoption and the decision-making process?

Coping appraisal is the second component that defines PMT, focusing on the ability to control a potential threat. Cyber insurance is evaluated as the possible solution to deal with cyber risks. Therefore it is important to know if companies perceive the usefulness of adopting it, or if they prefer other options. Similar with SQ3, the type of influence of the elements in the coping appraisal process are evaluated as well as the role during the decision-making process.

5th sub-question

SQ5: What are the drivers and impediments for SMEs to get cyber insurance?

After data gathered from the interviews is coded and analyzed, sufficient information will be available to identify the main drivers and impediments SMEs have when acquiring cyber insurance. Answering this question together with SQ3 and SQ4 will help to define a more accurate decision-making model.

1.4. Research methodology

Three main research methods were applied to answer the research sub-questions: literature review, semi-grounded theory techniques and interviews. Figure 1.1 shows the overview of the sub-questions and corresponding methods. The following paragraphs detail their relation.

Research question:
What decision-making process do SMEs follow to acquire cyber insurance?

	Sub-question	Methods
1	How does PMT explain a companies' need for cyber insurance?	Literature review
2	How can PMT be implemented in a decision-making model describing companies adoption of cyber insurance?	Literature review
3	How does threat appraisal influences cyber insurance adoption and the decision-making process?	Semi-grounded theory techniques, interviews
4	How does coping appraisal influences cyber insurance adoption and the decision-making process?	Semi-grounded theory techniques, interviews
5	What are the drivers and impediments for SMEs to get a cyber insurance?	Semi-grounded theory techniques

Figure 1.1: Research questions and methods to answering them

Literature review

Cyber insurance sector research is necessary to start with this study. Though cyber security as a general topic has been widely studied, for instance, the type of strategies used to mitigate botnets (Dupont, 2017), governance mechanisms in cyber security (Van Eeten, 2017) and cyber risk management (Hovav & D 'arcy, n.d.) just to mention a few, it is not the case for cyber insurance and most recent reports show this (e.g., (PwC, 2015)). Since the goal of the study was to investigate behavioral aspects of

cyber insurance adoption by SMEs, a clear picture of the state-of-art behavioral theories is performed to know how PMT is a suitable theory for the purposes of this research, and how it can be applied. After this, a literature review of existing decision-making models for insurance adoption will provide ideas about the way this process might look for cyber insurance adoption. Together with the literature review on cyber insurance, enough material is gathered to develop the questionnaire to be built for the companies. The previous research will answer sub-questions 1 and 2.

Semi-grounded theory

Semi-structured interviews serve as a primary source of information. The interviews differ depending on the stage the company is, it could be that the company already has a cyber insurance, is in the process of getting it, or decided not to get cyber insurance. The questionnaire is based on PMT theory, and brokers provide the contacts of the potential companies' representatives to interview. After the data is collected from the interviews, a qualitative analysis is conducted using techniques from semi-grounded theory approach such as: treat everything as data, immediate and continuous analysis, coding and group coding (Stol et al., 2016). More features exist (it is worth to mention theoretical saturation), but due to time constraints, it is not possible to apply grounded theory in full as proposed by the authors. Because of this, it is more convenient to refer to this method as semi-grounded theory.

Grounded theory is conceived initially to allow inductive generation of theory from data that has been systematically obtained and analyzed, instead of testing or validating the existing theory (Stol et al., 2016). Because of this, when grounded theory is meant to be used, the research questions should not make too many assumptions. Then, to answer research questions, data collection should come from primary research and collection techniques like semi-structured interviews, focus groups and participant observation (Willig, 2008). Acknowledging the use of this method, the literature review was meant to be neither extensively nor exhaustively. This step was done intentionally by seeing grounded theory from Charmaz' constructivist point of view, which highlights the need to do a literature review contrary to Glaser's vision.

Semi-grounded theory will assist in answering sub-questions 3, 4 and 5 by providing the techniques for detecting the elements from PMT that influence companies' decisions for getting cyber insurance.

Discussion, conclusions and reflection

After answering all the research questions, sufficient information will exist to address the main research question **"What decision-making process do companies follow to acquire cyber insurance?"**. A first stage will consist in defining the model for cyber insurance adoption product of the research and providing the conclusions of this research. Then, recommendations could be proposed for researchers wanting to conduct similar studies, and to the market side to improve products and services. A reflection on the results complements the final chapter of the thesis, followed by proposals for future research in different aspects that are out of the scope of this thesis.

Constraints on data gathering and scope

Reliability and validity are the primary concerns when gathering data from interviews. The interviews to be made with the companies' representatives should guarantee a degree of reliability, but the possibility of not getting the answers from the right person (e.g., that the company representative does not possess enough knowledge about the topic) could affect this aspect. The way to deal with this and avoid inaccuracies from data collection is by requesting the participation of representatives involved in the decision-making process for cyber insurance adoption, and by gathering various participants per type of scenario. The scenarios are introduced later in Chapter 4.

Validity is inherent within interviews because open questions allow the interviewee to provide answers according to what they consider more accurate. For instance, answers could be biased towards showing less responsibility for the company security role inside the cyber security ecosystem. To mitigate this problem, an immediate and continuous analysis was conducted, based on semi-groundes theory. This analysis started with a literature review and continued with the sampling and comparison of answers between the data gathered. Moreover, the author should avoid giving examples of responses since this could prevent the appearance of a grounded response. Finally, anonymity is considered to strength both reliability and validity aspects. Cyber insurance is still a new concept and companies could feel themselves being part of a beta product testing.

Regarding the scope of this thesis, the companies to be interviewed are small and medium-sized Dutch companies, which contacts are mainly provided by brokers offering cyber insurance and in some

cases, sectorial organizations. Both options are chosen to increase the participation rate in this research. In this way, a bias of only choosing those companies where a point of contact already exists or with whom it is believed more insights could be gathered is avoided.

1.5. Scientific and societal relevance

Cyber security is far from being an understood problem. The decentralized environment where it operates makes this practice even more difficult. The way this thesis will provide scientific value is by developing a model to understand how companies decide to transfer cyber risks into a third party. The cyber insurance market is widely studied concerning the demand and supply perspectives. It is still not clear what are the different reasons that make a company feel convinced it is the best way to protect themselves and mitigate (Franke, 2017) the effects of potential cyber attacks. Meland (Meland et al., 2017) did a similar study concerning interviewing the demand side, but it is conducted by looking only to uncertainty aspects like products, process, and support.

This research takes into account the different stages a company is at whether it is considering getting cyber insurance to identify diverse aspects that guide them in its decision. Additionally, the analysis of this process with a behavioral theory perspective will include the rationality that exists when companies are making decisions under risk, and at the same time, it will study aspects of irrational behavior present when these type of decisions are made. The use of semi-grounded theory works perfectly due to the lack of research on the topic and the lack of public information, which is one of the premises for using grounded theory: ”avoid bias in information and generate theory that accounts for a pattern behavior” (Stol et al., 2016). Though time constraints do not allow for the following of classic grounded theory process, it gives enough basis to extract useful information from the interviews that will finally help to describe the theoretical model of decision-making in companies to adopt cyber insurance.

From the societal point of view, a poor perception of cyber security can have two significant impacts: economic and low adoption of digital services. For the first a study by McKinsey&Company can be mentioned, where it is established that if cyber attacks continue increase in severity (as it has been the case), trust in the economy might be affected, causing global impact of up to $3 trillion by 2020 (Chinn, Kaplan, & Weinberg, 2014). For the second, discussions about how to connect the next billion people are essential since this means bringing Internet access to people at a lower social level, therefore, a poor perception of security on the use on digital technologies would make this task more difficult and also have an adverse effect on already active users (BPF Cybersecurity, 2017). Since SMEs count for almost 65% of the total number of employed people in the Netherlands (The European Commission, 2017), the impact they can create related to increasing cyber security awareness is enormous, and cyber insurance adoption is a possible way to deal with this concern.

1.6. Thesis structure

The structure of this document reflects the structure of the methodology. As has been explained, not much research exists in this field, therefore the way to approach the problem needs to be carefully documented. Chapter 2 explains the methodologies used and the way research questions will be answered; Chapter 3 provides an extensive overview of the theoretical foundation of this research, based on PMT, the business process for acquiring cyber insurance and other decision-making models for insurance purchase; Chapter 4 explains the way semi-structured interviews were prepared, the selection of participants for the interviews, and the coding process to analyze the data gathered from the interviews; Chapter 5 shows the results from the semi-structured interviews; Chapter 6 discusses the results to propose a decision-making model for cyber insurance adoption, present the conclusions of the research, and provides recommendations for researchers and the industry; finally, Chapter 7 is a reflection on this thesis and provides potential future research approaches. Figure 1.2 shows a preview of the thesis outline.

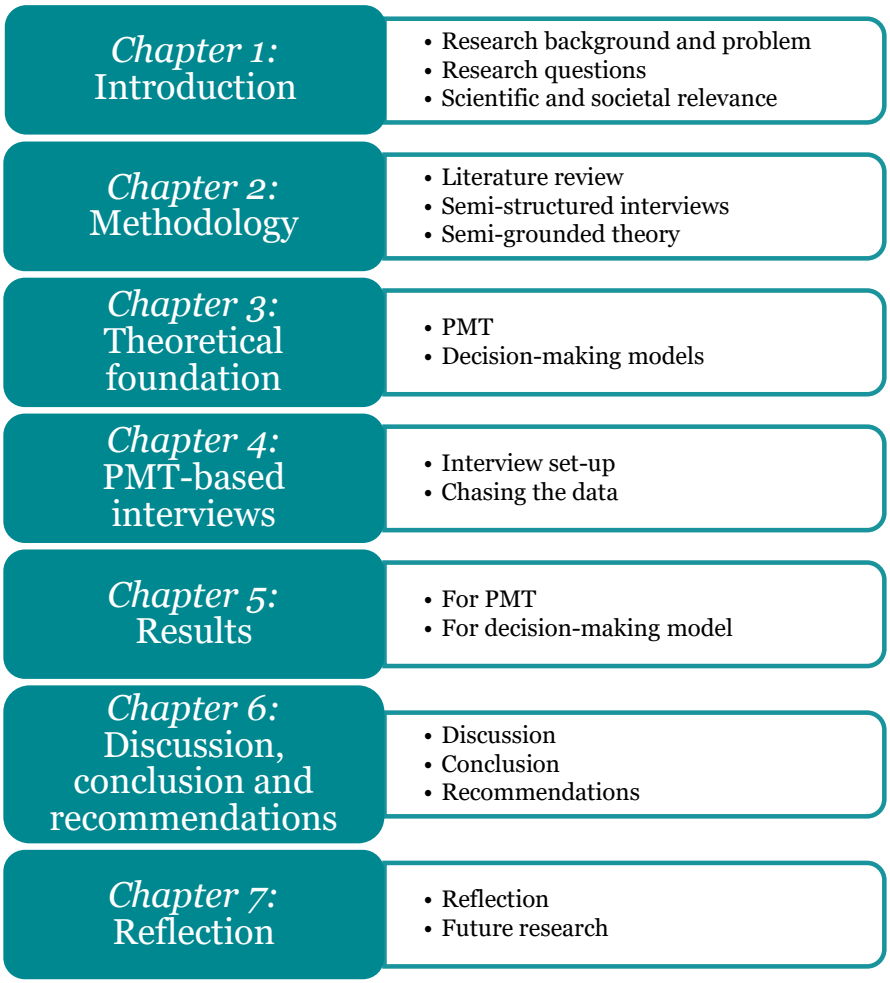


Figure 1.2: Thesis outline

This chapter proved that research about cyber insurance adoption for SMEs has not been widely studied even though these companies represent a significant player in the economy of the Netherlands. Cyber insurance has been mainly acquired in the U.S. but in the Netherlands it is still a new product. Because of this, empirical research based on semi-structured interviews is an appropriate way to gather data to analyze it then using semi-grounded theory techniques. An interesting approach that will be used in this thesis is based on PMT to study the non-rational aspects involved in the decision-making process to get cyber insurance. The chapter presented the sub-research questions that will help to answer the main research question "What decision-making process do SMEs follow to acquire a cyber insurance?"

2

Methodology

This chapter outlines the methods used during this research, which are literature review, semi-structured interviews, and semi-grounded theory techniques. Literature review helps the reader to understand why PMT was chosen among other behavioral theories; the reasoning to select semi-structured interviews as the primary source of data gathering; and the way semi-grounded theory is implemented. Finally, it is shown how these methods determine the path to answering the main research question and sub-research questions.

2.1. Literature review

Selecting the topics for literature review was not an easy task. The first topic that emerged was cyber security incidents to show the growing tendency in periodicity and impact. Nevertheless, the topic is already described in several pieces of research about cyber security. Even if not many people know the exact details with regards to dates, targets, and financial losses, it is not difficult to acknowledge the growing tendency of cyber security incidents. Then, although this information is not the main focus is important to have it as a precedent about the impact cyber attacks can cause. After having enough data to describe the tendency, a literature review about cyber insurance was made. One of the first things to notice is that there is broad research from the supply side of cyber insurance (e.g., (Tøndel, Seehusen, Gjære, & Moe, 2016; Franke, 2017; Woods et al., 2017)) as well as mathematical and game theory models for node behavior in a network, and insurance policy design (e.g., (Yang & Lui, 2014; Hayel & Zhu, 2015)). After this, it was clear that the research for the demand side is not prevalent and even less for SMEs in the cyber insurance market. Regarding empirical research, the literature review shows that the main subjects of study are the insurance companies and the executives in a C level position[1].

Due to the lack of research in the demand side, it was determined that the focus should be on SMEs and the final goal is to know the decision-making process followed in determining whether they get or not cyber insurance. The next step in the literature review was to research how companies make decisions. Cyber insurance decision-making process in big companies can be long where different departments and investors play a role (e.g., (Bandyopadhyay & Shidore, 2011) and (Srinidhi et al., 2015)), but the decision-making process changes depending on the size of the company. Because of this, research about behavioral theories was investigated since these theories are related to processes followed by individuals. Then, if interviews with SMEs' representatives about the decision-making process for cyber insurance are to be made, they could be closely linked to the process discussed by these theories.

Several behavioral theories exist among psychology literature. The theories analyzed involve a decision-making process towards adopting a product, and these are as follows: technology acceptance model (TAM), theory of planned behavior (TPB), and protection motivation theory (PMT).

[1]Corporate titles given to persons to show what duties and responsibilities they have, most common examples are the CxO titles like CEO, CIO, CISO, etc.

Since the late 80s, the use of computer-based tools and the advent of the Internet were reasons to study why people would accept or reject these systems. In this context, the TAM was introduced by Davis in 1986. The theory explains the perceived usefulness and perceived ease of use as part of an individual's behavioral intention to use a system (Davis, 1986). Figure 2.1 shows the model. This theory is focused on technology acceptance but it does not help to identify the user's decision-making process in every sector (e.g., (Sun, Wang, Guo, & Peng, 2013) makee a case for healthcare sector). Besides, the theory lacks the integration of human and social factors (Legris, Ingham, & Collerette, 2003). Moreover, even that the use of specific technologies are necessary to protect from cyber attacks the objective of this research is focused on cyber insurance, which is not perceived as a technology in the context of this theory.

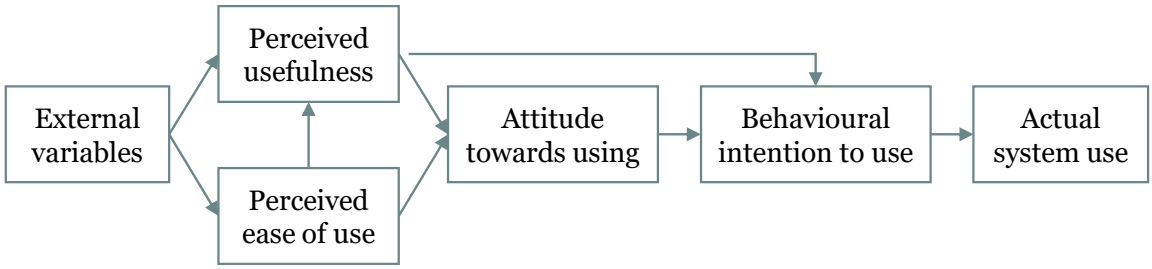


Figure 2.1: Technology Acceptance Model by Davis (1986)

Another theory related to technology acceptance behavior is TPB. Ajzen proposed the theory to predict and explain human behavior in specific contexts where the central factor is the intention to perform a behavior (Ajzen, 1991). The original model dates back to 1985, and it can be seen in Figure 2.2. This theory can explain individual behavior, but it fails to identify a perceived sense of danger to take protective measures. In this sense, cyber insurance is selected to cover potential losses related to a cyber attack, and this decision comes from the perception that a cyber attack is a potential danger for him or the company. Then, TPB is not enough to explain the decision-making process for cyber insurance adoption.

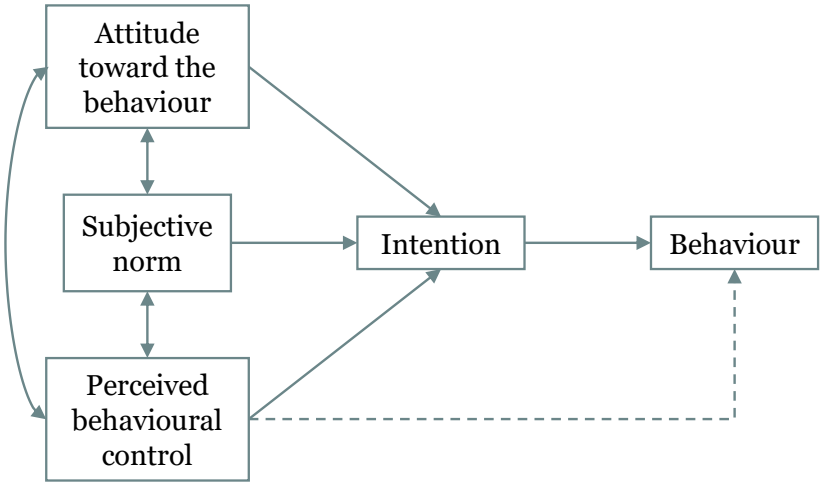


Figure 2.2: Theory of Planned Behavior by Ajzen (1985)

Finally, PMT, as it will be explained in detail in the next chapter, has certain characteristics that make it suitable to analyze the decision-making process to select cyber insurance. PMT considers external sources of information (a significant point considering that not all companies are expert in cyber security and external sources of knowledge can be influential), its starting point is the perception of fear, and is the only behavioral theory considering the costs. Regarding the last point, the literature

shows that costs are an essential factor when getting cyber insurance (e.g., (Meland et al., 2017) and (OECD, 2017)).

Moreover, the analysis of the behavioral theories is done with the focus of establishing how to apply the theory to the future decision-making model for getting cyber insurance. Therefore, it was necessary to analyze the elements that each theory could provide for it. In this sense, PMT is the best choice due to the aspects indicated in the previous paragraph and the separation of the factors forming the cognitive process, which provides an approach to later delineate a decision-making model.

A point between the literature review and the semi-structured interviews is the identification of the existing business process to acquire cyber insurance. The business process is used to identify the different stages the company is involved in when the proposal of the cyber insurance is presented, as well as to know the participating actors. As it was showed in Chapter 1, the type of companies that have got cyber insurance are large companies instead of SMEs. Managers in large companies are commonly characterized as being risk-averse, adhere to accepted norms, and predictable in their decision-making (Busenitz & Barney, 1997). Then, the business process foresees a structured behavior by the actors and is mainly applicable for large companies. Nevertheless, it is a starting point based on existing literature, and it will also be validated with experienced actors (mainly with brokers) to acknowledge how close it is to a decision-making process in real life.

2.2. Semi-structured interviews

Interviews are a way to collect data about the main reasons why an SME decides to get or not to get cyber insurance. By doing interviews, information about the context where decisions were taken can be gathered, and as Seidman (Seidman, 2006) indicates, through interviews it is possible to put the persons behavior in context. Moreover, the use of semi-grounded theory requires the data to arrive from primary sources like is the case for semi-structured interviews. Since literature review has shown that the research focused on SMEs is scarce, and the cyber insurance market in the Netherlands is still new, finding companies able to explain their decision-making process is not an easy task. Therefore, the narrative of how the interviews are designed is important not to make feel the interviewee overwhelmed. Wagenaar (Wagenaar, 2014) recommends three tasks to keep in mind during interview process, these are: 1) establish a working relationship with the interviewee, 2) keep analyzing the interview material to guarantee quality, and 3) help the interviewee developing the material. The way to consent with this is to follow these rules:

- Provide a consent form to guarantee the anonymity of the interviewee and explain the research objectives for which the data will be used. This consent form is provided before time and date for the interview have been arranged so that the interviewee has time to read it.
- Before starting the interview, indicate again the objective of the research together with the introduction of the interviewer.
- During the interview, the research must avoid expressing opinions as well as not making closed questions to avoid patterns and allow the interviewee to develop the material in their own terms.
- Know the questionnaire by heart to allow interaction between questions and ask simple questions at the right moment to allow the interviewee to provide more details. This will also help the interviewee not to feel in an inquisition.

Chapter 3 will explain the theoretical foundation of how the questions were formulated to comply with the objective of having a clear narrative. After that, pilot interviews were done with an expert in cyber security at TU Delft and a CYBECO[2] partner from the insurance domain. The pilot interviews aimed to test the clarity of the questions, calculate the duration of the interview, and serve as a probe that the most important aspects regarding decision-making to get cyber insurance are included. Later, Chapter 4 explains how the interviews were arranged.

[2]CYBECO is the Cyber Security Project funded from the European Union's Horizon 2020 Research and Innovation programme, TU Delft among other actors participate in this project. For more information go to: https://www.cybeco.eu/

2.3. Semi-grounded theory

Grounded theory was originally developed by Berney Glaser and Anselm Strauss in the late 60s but has evolved into different versions, having predominantly the classical (or Glaserian), Straussian and Constructivist grounded theory versions. Each one of them differs on how it starts to be used, how should the literature review be held, how to do the coding, what questions should be done during the analysis and, the philosophical influence they are based on. Moreover, the principles these three versions have in common are that categories should emerge in an ongoing process of data analysis, coding should be employed, use theoretical sensitivity to conceptualize and establish relationships between different concepts, and execute a constant comparison of data.

After data is obtained from the interviews with SMEs' representatives, it is analyzed and used to build the theory around the aspects that motivate or discourage companies to get cyber insurance, and the decision-making model they follow. All interviews were recorded and the participants consented to this and the use of the data they would provide. The anonymity of the company they represent and their personal information is preserved at all times. The recording allowed the interviews to be fully transcribed and analyzed using Atlas.ti software, which is widely used in qualitative data analysis. This software allows code quotations, group codes, relates them, and provide convenient tools to analyze codes frequency and co-occurrence in different artifacts.

A connection between the development of semi-structured interviews and the use of semi-grounded theory is the concept of theoretical saturation as a criteria measure in qualitative research and specifically, in grounded theory. According to theory, this concept indicates the stopping point for collecting and analyzing data (Stol et al., 2016). Translated for this research would mean the point where no more interviews should be made. Chapter 4 explains in detail how the interviews were arranged, but it is important to mention first, since research about cyber insurance adoption among SMEs has only just started to be made, it is expected every interview will provide new and in-depth knowledge on the topic. Secondly, three scenarios are described for the companies, then an equal number of interviews per scenario will try to be collected. Third, in order to get the interviews, the research is highly dependent on the collaboration of the brokers and the SMEs.

Finally, this research is done within a fixed time schedule. Taking into account the previous, theoretical saturation in this research is defined by a combination of all the mentioned points. This does not mean that the concept of theoretical saturation is not observed, since according to (O'Reilly & Parker, 2012), "the variability between categories are explained and the relationships between them are tested and validated and thus a theory can emerge", which it is the purpose of this thesis, but under the constraints defined by time and accessibility to the sources. To have an overview of how the working process for this thesis is done, Figure 2.3 shows the course of the research, indicating the steps where the sub-research questions are answered.

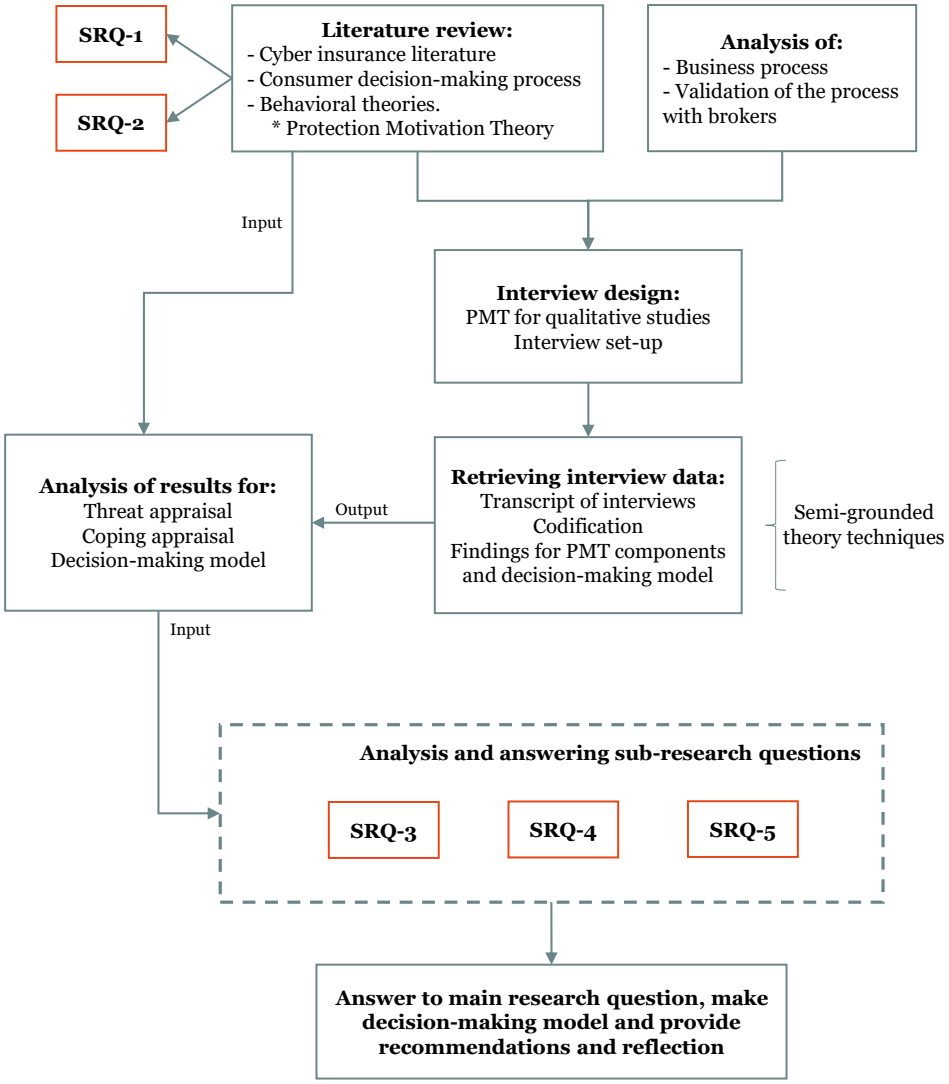


Figure 2.3: Research flow diagram

In this Chapter, three methods are described: literature review, semi-structured interviews, and semi-grounded techniques. Section 2.1 described the literature review focused on crucial cyber security incidents (in terms of their impact), cyber insurance adoption, cyber insurance decision-making, behavioral theories, and PMT. Section 2.2 indicates why semi-structured interviews were chosen as the main source for data gathering. Finally, Section 2.3 introduces the semi-grounded theory and the techniques adopted from this theory to analyze the data gathered from the interviews. It also states the researcher's stance on theoretical saturation concept for semi-grounded theory in this thesis.

3

Theoretical foundation

This chapter presents the theory needed to start preparing the decision-making model for cyber insurance adoption. First, the PMT is described in detail in Section 3.1. PMT is the core of this research since it is the backbone for the type of data that will be later gathered. Then, in Sub-section 3.1.1 an adaptation of PMT elements to the cyber insurance context is provided, as well as an explanation of why it is useful to apply such a theory to this research. Apart from PMT but acting as an important complement in the theory for cyber insurance adoption, Section 3.2 presents two processes, the business process and the insurance adoption process. First, Sub-section 3.2.1 introduces the business process to get cyber insurance, where a logical set of steps as expected to be in a business process is presented. This process represents the common rational behavior any organization has. Then, Sub-section 3.2.2 presents the existing literature for cyber insurance adoption and insurance consumer behavior to understand that the business process lacks the inclusion of elements representing the irrational behavior presented when decisions under risk conditions are made. After this, Section 3.3 brings together PMT with the insurance adoption process to understand how they interact and demonstrate that PMT covers aspects presented in this process. Finally, in Section 3.4, the answer to the first two sub-research questions is provided.

3.1. Protection motivation theory

PMT was originally developed by Ronald W. Rogers in 1975 to explain the effects of fear appeal towards health issues. Since then, researchers have highlighted the importance of differentiating emotional responses from cognitive responses. In the face of a threat, an emotional response would lead an individual to avoid the threat, while the cognitive response would lead him to avert the threat (fear control versus danger control) (Leventhal, 1970). PMT links these two aspects to antecedent communication stimuli and states that a fear appeal initiates the cognitive appraisal process where the outcome will be a protection motivation measure. The measure can be either to continue with the current behavior, or to adopt a preventive behavior.

PMT is developed along two processes based on the cognitive process people follow to evaluate threats (the threat-appraisal process) and selecting the alternatives to handle this threat (the coping-appraisal process). Later in 1983, Rogers included a couple of additional elements to his original model, the reward and self-efficacy elements. An important aspect about PMT is that it not only considers the internal process a person follows to make a decision, but it also takes into account the environmental factors to enhance the encouragement or discouragement to adopt protective measures. Figure 3.1 displays PMT's model, a definition of each component is provided afterward.

- ***Sources of information.*** This component is comprised by the environmental and intrapersonal sources of information elements. It provides suggestions regarding potential victimization threats, potential protective options, and reasons why the individual should or should not engage in a given protective response (Clubb & Hinkle, 2015). Overall, this component offers general information about existing threats and the available ways to deal with it. Floyd (2000) exemplifies the two variables as follows:

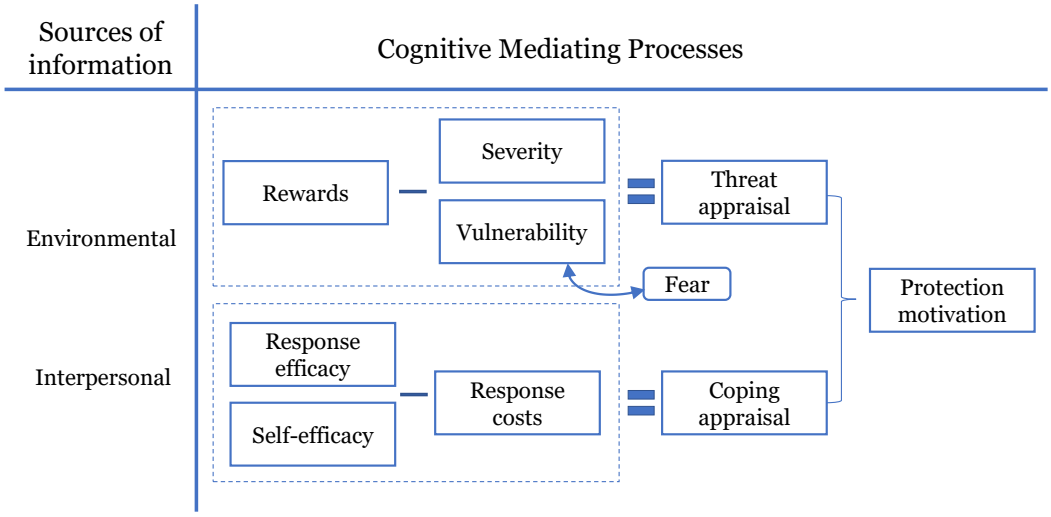


Figure 3.1: Protection motivation theory model

  - Environmental sources of information: verbal persuasion and observational learning.
  - Intrapersonal sources of information: personality aspects and feedback from prior experience.

- ***Threat appraisal.*** The component that evaluates the maladaptive behavior formed by the elements of rewards, severity, and vulnerability. In this stage, the person analyses the consequences of not engaging in protective actions against the severity of the threat. The elements of severity and vulnerability create a positive effect towards taking an adaptive response because they indicate the extent to which a person believes that a threat is severe, and the possibility to be affected by this threat (Posey, Roberts, Lowry, & Hightower, 2014). On the other hand, if the analysis of the rewards element is found to be higher than the severity and vulnerability elements, it is more likely that the person will continue with the maladaptive behavior. Then, the rewards element encourage the person to expose a certain type of behavior knowing that threats exist around this action.

- ***Coping appraisal.*** This component evaluates the adaptive response by considering the available responses or measures that could protect a person from a threat. The factors that the person will analyze are related to his belief of how capable he is to implement the protective measure (self-efficacy element), how effective will the measure be (response efficacy element) and the costs associated (response cost element) (Floyd et al., 2000). If the costs have a higher evaluation than the potential benefits for engaging in the protective behavior, the person will likely not consider selecting the adaptive response. In PMT, the response costs can be any costs like social, financial, time or effort.

The threat appraisal and coping appraisal processes are nourished by the environmental and intrapersonal sources of information. The final assessment by an individual follows the summation of all the components to decide if he will initiate, continue or inhibit the adaptive response. These two possible scenarios are accomplished if the considerations according to Table 3.1 occur.

3.1.1. Why PMT for cyber insurance?

Research on protective behaviors has been mainly (and originally) done for health issues like smoking and cancer prevention. Later it started to be expanded to other topics like prevention of nuclear war (Axelrod & Newton, 1991), food safety (Schafer, Schafer, Bultena, & Hoiberg, 1993), and information security (Boss, Galletta, Lowry, Moody, & Polak, 2015). In this sense, we can draw similarities between the research done for information security with the cyber security context. Protective behavior research in the information security sector has been focused on the personal and working areas due to the

Inhibit the adaptive response	The potential threat is not serious The potential protective response will not be effective The costs are too high
Initiate or continue the adaptive response	The potential threat is serious enough The potential protective response will work The potential protective response is affordable

Table 3.1: Role of PMT elements in an individual's protection decision

violations of information and privacy security that has been happening. The objective of this type of research is to motivate individuals and organizations to improve the protection of information assets.

PMT looks into the reasons that guide people to protect themselves, or not against a detected fear. Regarding cyber security, the fear of a company of being affected by a cyber attack should first exist to then consider potential solutions to protect against it. Previous research in the information security field about the use of PMT (Woon, Tan, & Low, 2005; Gurung, Luo, & Liao, 2009; Lee & Larsen, 2009) gives an excellent background to explain the protective process individuals follow when they believe themselves or their organizations are susceptible to security threats. Woon (2005) tries to find differences between users that decide to secure their home wireless network and those who do not, by means of a survey based on PMT. Gurung (2009) finds that if end users perceive they have sufficient knowledge to implement anti-spyware tools, they will be more keen to use them. Lee (2009) studies manager's behaviors in SMEs to get anti-malware software for their companies, finding different aspects from both threat and coping appraisal play a role in the manager's decision.

Taking the definition provided in the previous section about the PMT components, is now adapted in the context of cyber insurance. Moreover, the adaptation applies to both the PMT components and elements. This will help to develop further the questionnaire that will be built for the SMEs representatives.

- ***Sources of information.*** The suggestions regarding potential victimization threats, potential protective options, and reasons why the company should or should not engage in getting cyber insurance (Clubb & Hinkle, 2015). The two elements comprising this component in the cyber insurance context include:
  - Environmental sources of information: verbal persuasion like conversations with colleagues, clients or other companies about cyber insurance; observational learning like knowing a company that has suffered a cyber attack (beyond what is reported in the news), or knowing companies adopting cyber insurance.
  - Intrapersonal sources of information: personality aspects like the professional background, role in the company and knowledge about cyber security; feedback from a prior experience like directly witnessing a cyber attack.
- ***Threat appraisal.*** The component that evaluates the maladaptive behavior. Its elements analyzed from cyber insurance perspective can be described as follows:
  - Rewards is comprised of extrinsic and intrinsic rewards. Extrinsic rewards like other companies not adopting cyber insurance, avoid an expense that is conceived as unnecessary, the absence of sanctions for continuing with the maladaptive behavior. Intrinsic rewards like the belief that it is not a useful measure because the likelihood of being affected by a cyber attack is low, the fact that the measure is not included in the company guidelines, or to project an image that the company is capable of protecting by itself.
  - Threat severity is the degree of harm from the unhealthy behavior. Therefore, if a company thinks it is susceptible to attack, it could also perceive which are the attacks they are most afraid of, and how severe the consequences would be.
  - Vulnerability is the probability that a company will experience harm. Therefore, if the company believes it is susceptible to a cyber attack, it could identify which activities performed by the company are of interest to attackers. The element could also be translated into the type

of precautionary measures the company has taken with its IT security to prevent potential cyber attacks.

- ***Coping appraisal.*** The component that evaluates the ability to cope with and avert the threatened danger. In the cyber insurance context, the coping appraisal elements are described as follows:
  - Response efficacy is the belief of the company that adopting a response in the form of cyber insurance will work. This can be translated as the expectations the company has about how the insurance will work as well as how effective will be the support from the insurer or broker.
  - Self-efficacy is the perceived ability of the person to carry out the adaptive response. For instance, how much data does the person have about cases where cyber insurance can be used or how has the company been dealing with cyber attacks.
  - Response costs are any costs associated with getting cyber insurance. The first cost to consider is the financial cost, meaning the premium price. Negative costs could also be considered, like lowering the level of security because the company knows that in the face of an attack, a third-party will take care of it.

3.2. Decision-making models for insurance purchase

In this section, two different types of processes are analyzed. First the business process to acquire cyber insurance. The business process was analyzed based on literature review and input from experts, later reviewed with brokers offering cyber insurance and cyber insurance providers. Second, processes to buying cyber insurance and any other type of insurance are analyzed. The elements that should be considered in the present research and the questionnaire to be made were identified.

3.2.1. Business process to acquire cyber insurance

The importance of the business process is to identify the main actors and the regular steps followed. As it was stated in Chapter 1, cyber insurance market is predominant among large companies. Then, the business process to be described is the one regularly found in this sector.

Actors can be studied from a network perspective. As stated by De Bruijn (2012), "in a modern society, everyone depends upon everyone else", and this dependency can be translated in a network. A company can be studied as a network, as well as the cyber insurance ecosystem. To do this, actors have to be identified as the nodes of the network. The interaction of the actors have effects in the network, and since the interests of each actor are different, they can harm or support each other. Then, practical information is needed to know the actors' perspectives in the cyber insurance ecosystem because when a decision-making process occurs, different actors (or stakeholders) are involved.

The stakeholder analysis technique proposed by Enserink (2010) requires to formulate the problem from a problem owner perspective or an analyst perspective. In this case, a problem owner perspective is chosen since the objective is to know the decision-making process followed by SMEs. The next step of the analysis is to make a list of the actors involved. The list could be created in different ways, but it should be limited and focused on the formulated problem. According to Enserink (2010) different approaches can be used, the imperative approach is used to identify the actors that perceive a direct consequence regarding the existence and implementation of cyber insurance. After the list of actors is done, the mapping of their relations can be identified. A way to show it is with a context diagram, which helps to set the system scope (Ian Faulconbridge & Ryan, n.d.).

Figure 3.2 shows the context diagram for this problem, where straight lines indicate a direct relationship between the actors, while dotted lines indicate informal relations between them. The key interfaces and influences are labeled to illustrate the impact specific interactions have on the system.

- EO1: The insurance market is the primary beneficial actor of companies getting cyber insurance. Therefore they will try to influence the companies' mindset about the necessity of the product and its benefits.
- E02: Since the number of personnel SMEs can have is limited they tend to outsource activities for which they are not expert or they do not have the people to carry them out. This is the case for IT security, SMEs rely on the advice and services these companies give.

- E03: Insurers have found support to provide cyber insurance in IT security companies. Some insurers provide services from these IT companies as part of the cyber insurance coverage like monitoring and support when a cyber attack occurs.

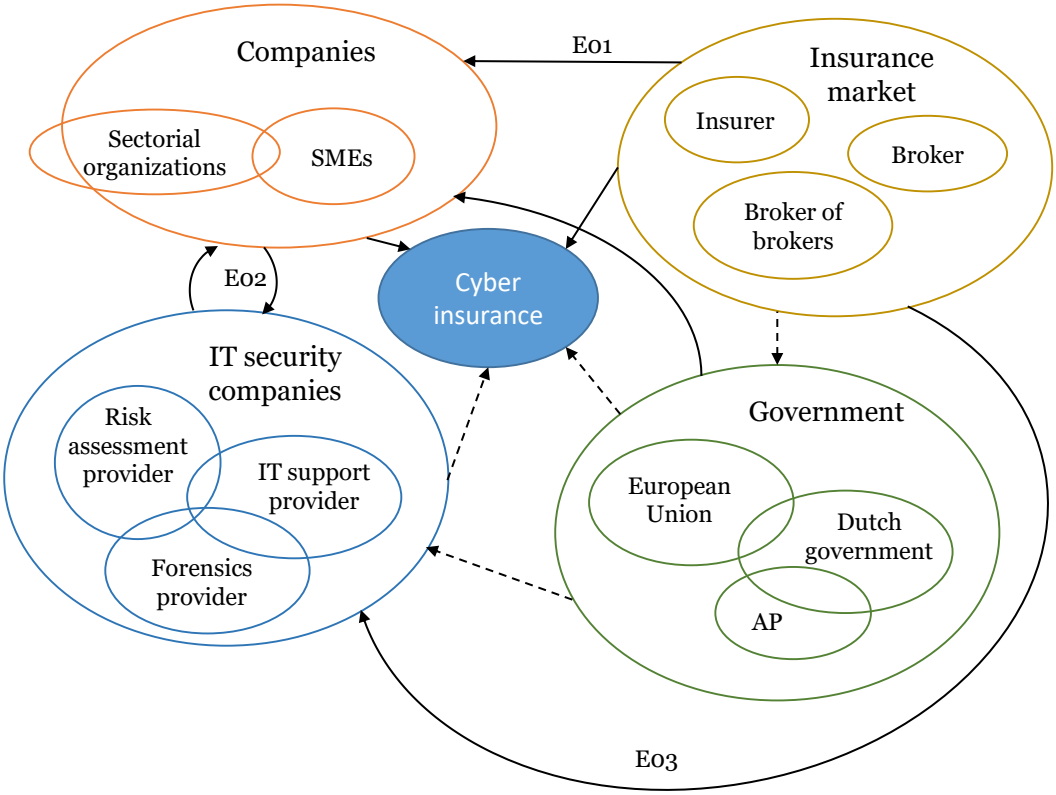


Figure 3.2: Cyber insurance context diagram

The detailed explanation of the rest of the interactions and the description of the actors is in Appendix A. The purpose here is to show the main actors participating in the process to acquire cyber insurance and how they interact to identify the tasks they share. From the interfaces E01, E02 and E03, three main group of actors are identified: companies, insurance market and IT security companies. For the business process, specific actors can be extracted from these groups. From the companies group, SMEs are the main actor since they represent the company considering getting cyber insurance. From the insurance market group, the insurer and broker are chosen. The broker is the actor in charge of creating awareness about cyber risk and can offer different policy options to companies, while the insurer will later play a role when is selected by the company as the insurance provider. From the IT security companies, the risk assessment provider is the most common actor participating in the process to acquire cyber insurance since it evaluates the company's level of security.

The business process is based on literature review, analysis of cyber insurance products and verification with experts like brokers and insurance companies providing cyber insurance. Figure 3.3 shows the detailed process where the participating actors are: 1) the company evaluating to get cyber insurance or not, 2) the broker, 3) the insurance company, and 4) the IT security company.

Before the process was formalized by the model in Figure 3.3, based on literature, the assumption was made that the actor starting the process to get cyber insurance was the company. However, as mentioned before, the literature is based on the process followed by large companies. After a couple of meetings with brokers, this assumption changed towards a practical point of view where the broker has a more proactive role in the SMEs market. The main reason for this behavior is the novelty of cyber insurance in the Netherlands since companies started to offer this type of insurance no longer than 5 years ago. Moreover, since local insurers do not provide cyber insurance in their catalog, the offering of cyber insurance still relies on international insurers. Then, in order for international insurers to promote

their products in a new market, they rely on broker of brokers (or managing general agent) to contact local companies and ”spread the word” about the need and benefits of having cyber insurance.

The process for getting cyber insurance does not differ drastically from the process of getting any other type of insurance. The company evaluates the need to have cyber insurance and notifies about this to the broker, then an interchange of information occurs to assess the level of security the company has. When the insurance company is selected, based on the information provided about the security level of the applicant, it can decide whether a risk assessment is necessary or not. If the risk assessment is necessary, the IT security company comes into play. Finally, when the company receives a policy offer, it has the opportunity to accept it or reject it. Overall, the process in Figure 3.3 illustrates the cycle from the broker creating awareness up to the decision regarding the contract proposal.

The importance of the business process is the confirmation from a theoretical (the literature review) and practical (interviews with brokers) point of view. Nevertheless, something to notice is that the process is mainly valid for large companies, and as stated by Busenitz & Barney (1997), in large organizations, elaborate policies and procedures are developed to assist managers in their decision-making, facilitating the complexity of the process through the use of these routines.

An adaptation of the process shown in Figure 3.3 from large organizations to SMEs can be seen in Figure 3.4. In this version, two actors participate instead of four, the SME and the broker. The elimination of the insurer corresponds to the fact that the interaction mainly happens between the SME and the broker, the insurer’s tasks are reflected in the broker. The IT security company is not presented because from the interviews, it was noted that a cyber risk assessment is rarely done during the process of acquiring cyber insurance. This adaptation shows a less developed process which is consistent with (Busenitz & Barney, 1997) arguing that small companies do not develop elaborate decision-making policies and procedures characteristic of large organizations. Similar to the model for large organizations, the process in Figure 3.4 illustrates the cycle from the broker creating awareness up to the decision regarding the contract proposal.

From Figure 3.4, three events can be distinguished. These events (identified by the circles with a thicker border) help to distinguish the three phases an SME is when the idea to get cyber insurance is brought to them:

1. The company is in the process of getting cyber insurance.
2. The company decides to get cyber insurance.
3. The company decides not to get cyber insurance.

The next sub-section will explain the findings of existing decision-making models to get cyber insurance and also decision-making models for the purchase of other types of insurances.

3.2.2. Cyber insurance decision-making process

The demand side for cyber insurance is companies. Then, if a company wants to get cyber insurance, who makes the decision? What kind of factors should be considered to get a product that in the Netherlands and for SMEs is still a novelty? PMT provides an approach of the factors that could be involved in the decision process but is not sufficient to construct the whole decision-making process. Since this is the case, a question comes next: What are the existing models?

In the context of cyber insurance, research on the main databases like Scopus and Web of Science using keywords such as ”cyber insurance decision making” and ”cyber insurance adoption” shows no more than 15 results, with many of them overlapping. This number of results is a first indication that not much academic work has been done for developing a decision-making process for cyber insurance. The three works presented in Table 3.2 have an approach to provide a decision-making process to select cyber insurance and to show different perspectives of what it means to develop such an outcome.

From the works presented in Table 3.2, it can be highlighted that (Bandyopadhyay & Shidore, 2011) looks into the decision-making process of sectors different from cyber security or information systems. (De Smidt & Botzen, 2018) indicates that since cyber insurance deals with cyber risk, a non-rational behavior might be followed by people in charge of deciding on getting the insurance due to the inexperience in this kind of risk events. Also, he makes an interesting point by indicating that emotional factors like level of concern, worry, and trust play a role at the same level to IT experts as to any other person with a lack of knowledge in the area. This statement makes it possible to consider

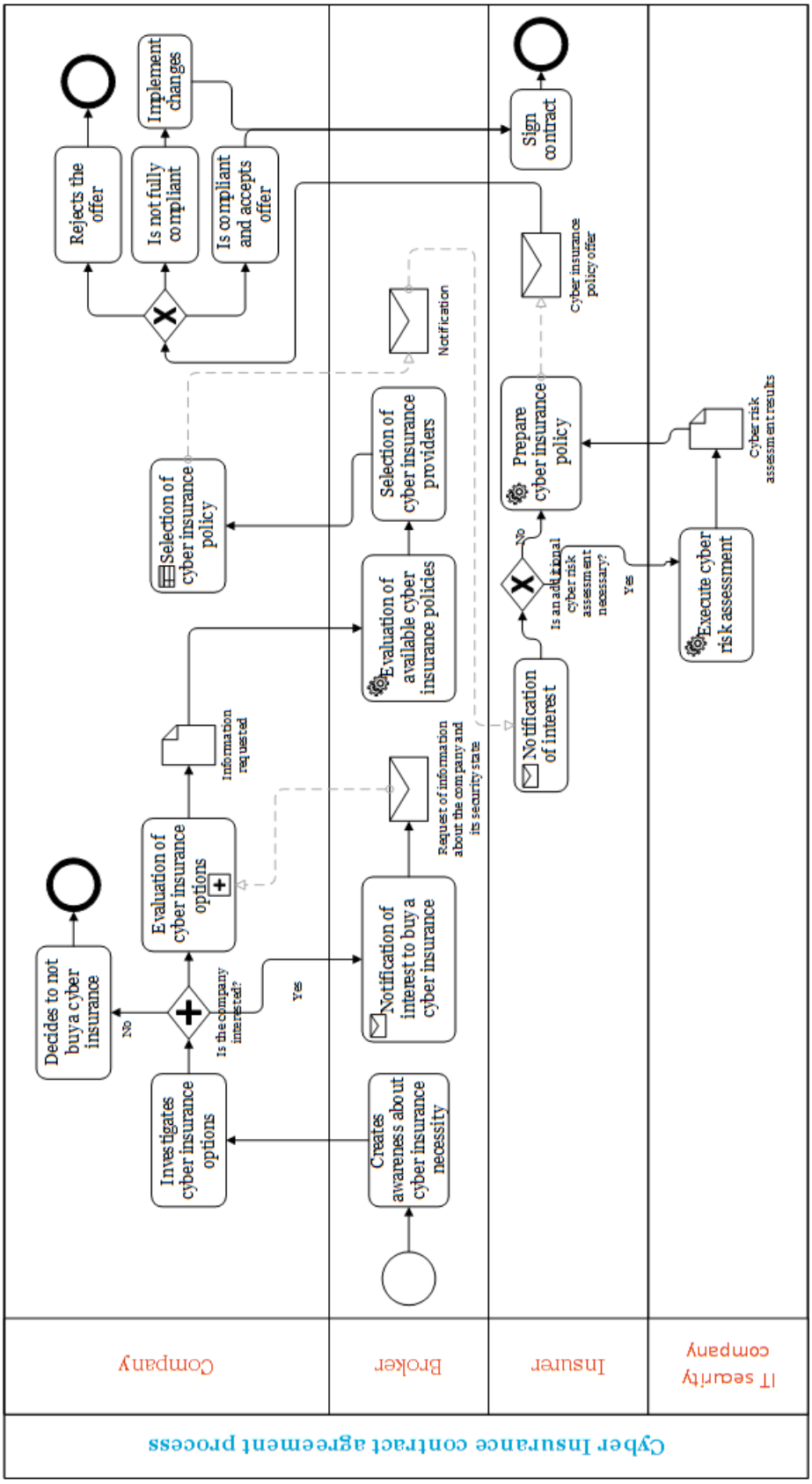


Figure 3.3: Cyber insurance contract agreement process

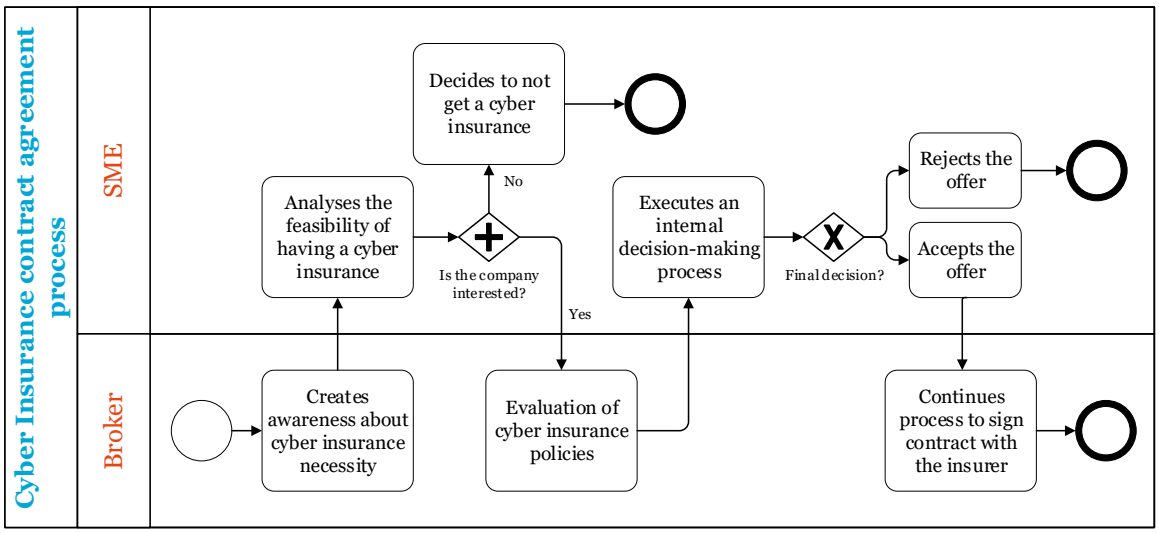


Figure 3.4: Condensed version of cyber insurance contract agreement process

the emotional factors applicable to any person in charge of deciding on cyber insurance, where an expert background does not make a difference. Moreover, since emotions play the same role among individuals with different level of knowledge, behavioral theories like PMT applied in decision-making processes can be implemented.

Since no decision-making model for getting cyber insurance in SMEs is found, the research moves to look into another type of insurer. A possible explanation for not identifying suitable models is that SMEs do not need a long process to make decisions, compared to larger companies. For SMEs, the decision-making process involves fewer people, and they do not have enough resources to hire external insurance and cyber security consultants if this is not related to the main company's business. Many examples can be found when looking for the decision-making process for any insurance, but the two works presented in Table 3.3 are the most relevant for this research.

The analysis by (Kunreuther & Pauly, 2018) is based on expected utility theory to find if the irrational consumer's behavior to buy insurance is based on emotions. If this is the case, Kunreuther (2018) indicates that it might be worth to explore the case where public policies could intervene to avoid this behavior and allow more accurate economic predictions. Other authors have also explored utility theory in the decision-making process to select insurance (e.g., (Song et al., 2010)). Implementing utility theory requires quantification and measure of feelings, and considers that individuals make a serious analysis of the different factors that should be involved in a decision-making process. For instance, in Kunreuther's (2018) paper, factors like changes in the occurrence probability of a hurricane, financial losses, premium prices are considered. To prove this theory, concise scenarios and concise answers are required, since the same scenario is presented to a sample of almost 2,000 individuals. The previous is mentioned to indicate the difference on sample size between quantitative and qualitative studies, where for a qualitative study like this aiming to interview SME's representatives, gathering that amount of data is not possible or necessary.

It is well proved that consumers do not always make rational decisions about buying goods. Gerd Gigerenzer says that people are bad at understanding probabilities, and the probability is necessary to calculate risks. He proposes to teach risk literacy to everyone to deal with this issue (TEDx, 2013). In this context is interesting to look towards Kahneman, who studied human irrationality and gave him a Nobel Prize in 2002. In his infamous book "Thinking, fast and slow" (Kahneman, 2011), he defined two modes of thought named "System 1", the fast, automatic, intuitive and unconscious mode, and "System 2", the slow, deliberate, analytic and consciously effortful reasoning mode. Without trying to explain in deep his research, Kahneman indicated that each mode has its own cognitive biases and his main advice is, in any situation you are, think first.

Another interesting work in the field of insurance consumer behavior was done by Ulbinaite (Ulbinaite et al., 2014) who defined a framework to represent consumer's purchase decision, including elements like the perception of need of insurance, the perception of affordability, previous experience with in-

Reference and description	Relevant aspects	Differences with this study
(De Smidt & Botzen, 2018) makes a study about individual perceptions of cyber risks to analyze the role behavioral factors play when professional decision-makers have to choose to get an insurance or not.	By making decisions under risk people deviate from rational behavior. An individual's intuitive decision process influences risk perceptions in the same way as can happen to experts. Perceptions individuals have about cyber risks matter when persons are taking decisions.	The focus is on big companies and experts either in risk management or insurance field, different from the focus of this research in SMEs. The measure of perceptions is done in a probabilistic way, therefore, asking questions to rank certain aspects between low and high, whereas this research follows a qualitative method.
Bandyopadhyay (2011) proposes a framework to draw the organizational process managers follow to decide between getting or not cyber insurance. He argues that the different backgrounds between IT managers and risk managers require both parties to communicate.	Descriptive and prescriptive models are analyzed to recognize aspects from IT and risk managers that should be included in the final framework. Descriptive decision making is based on bounded rationality, while prescriptive models have a realistic vision. The background research is focused in different decision-making models like industrial buying behavior, which indicates the possibility to apply research from different fields.	The focus is on big companies where the most common departments and managerial positions are recognized in order to identify the way they should interact and the level at which they should communicate. This structure is not found in SMEs, making the proposed framework inapplicable to these types of organizations.
Mukhopadhyay et. al. (2013) addresses security breaches in an organization from the technological and business point of view. He considers technical measures like perimeter security, security policy, and monitoring, and business parameters like organization's structure, budget, and culture.	Potential premiums an insurer could calculate are provided based on a calculation and modeling of an organization's cyber risk. The recommendation in the paper about getting an insurance or not is based on the actual state of an organization together with the financial resources it has are valuable to consider as input for this research.	The focus is on big companies, considering the interaction in the organization at the C managerial level. Moreover, the process requires to have in place vast and accurate amounts of data for all the parameters it recommends being included in the model since a Bayesian type methodology is used. The study is interesting in the way it chooses the variables for the model, but it differs in the sense that this research is not making quantitative calculations.

Table 3.2: Decision-making + cyber insurance literature research

surance products, consumer's life quality and a consumer's literacy. Figure 3.5 shows a condensed version of Ulbinaite's model. Compared to the model presented in (Ulbinaite et al., 2014), the block "Evaluation of insurance services" in Figure 3.5, represents the collection of steps explained in more detail in her work, but in no way change the meaning or purpose of the model.

The way the model is presented is as follows:

- Rounded rectangles represent the different steps a consumer might face. The term "might" is used on purpose. For instance, if the consumer is situated at the Consumer's life quality element, a decision after analyzing this element could be made, which is to decide not to get insurance.

Reference and description	Relevant aspects	Differences with this study
(Kunreuther & Pauly, 2018) focuses on the analysis of low-probability, high-consequence events like a hurricane. Explains the changes in decisions individuals have depending on the available information at the moment.	When a person wants to take insurance, emotions like reduction of worry and gain peace of mind play an important role. Regarding cyber insurance adoption, it would be interesting to find out if these kinds of emotions are present.	The analysis is made in different stages where the person decides to get an insurance or not to measure the level of feeling the person had at the moment. This study is not focused on measuring the person's feelings for getting cyber insurance.
(Ulbinaite, Kucinskiene, & Le Moullec, 2014) proposes a model to explain the different stages a consumer follows to purchase an insurance and evaluates the model using agent-based modeling to measure the impact of the different elements proposed in the model.	A clear and complex model is proposed to identify the multiple stages a consumer is when selecting insurance. The model identifies the elements and the flow the consumer follows to decide about a subsequent acquisition. Insurance consumer behavior theory elements are explained to form the suggested model.	The way to probe the possible applicability of the model is through a modeling tool instead of empirical research. The way the parameters are programmed in the model have an impact in the final results. For this research, the focus is on the proposed model and not on the results presented in the study.

Table 3.3: Decision-making + insurance literature research

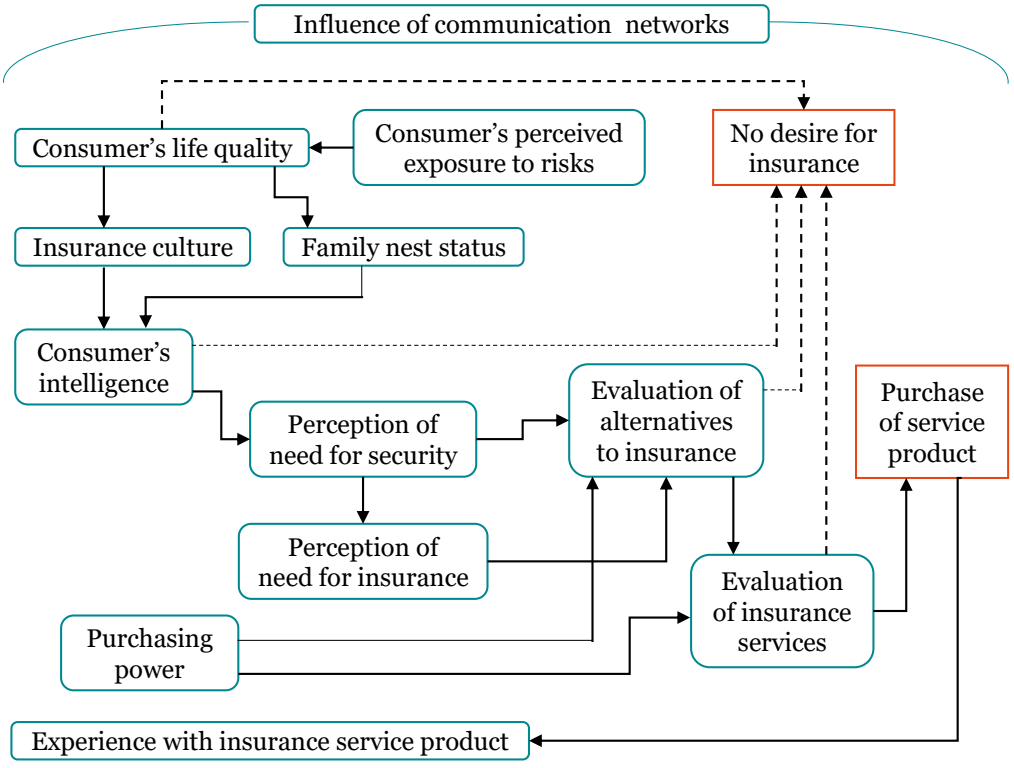


Figure 3.5: Ulbinaite's decision-making model for an insurance service product

Then, the consumer does not necessarily have to go through the process.

- The rectangles represent the two possible decisions a person could reach, either to get or not the insurance.
- Straight lines represent the path to be followed to get insurance.
- Dotted lines represent the path to be followed to not get insurance.

Ulbinaite's (2014) decision-making model is interesting since it can be widely applied to the purchase of any insurance. It is dynamic in the sense that at several points a person can take a decision without necessarily having to go through all the stages, and it considers the external network any human has, which can have an influence in different stages. Since the model in Figure 3.5 shows the elements Ulbinaite's model considers, next is a brief explanation of the element's characteristics. Something to keep in mind is that since Ulbinaite's model is developed for any insurance service product purchase, the explanation and examples provided are related with the acquisition of popular insurances like health or life insurance.

- *Influence of communications networks;* local networks like the family and social groups, and external network like channels of advertisement and sales.
- *Consumer's perceived exposure to risks;* probability of exposure to risks, available statistical data for the consumer.
- *Consumer's life quality;* analysis of present and future circumstances of the individual. For instance, if the consumer wants to get health insurance, he would consider his actual and future health status.
- *Insurance culture;* indicates the type of risks a person is exposed to and the amount of coverage he has for these risks.
- *Family nest status;* represents the person's stage of life and his responsibilities towards others if any.
- *Consumer's intelligence;* it consists of two aspects: 1) knowledge towards insurance, either from personal or external experience and education level; 2) aptitude towards insurance, consumer's risk awareness, and the ability to manage financial products.
- *Perception of need for security;* evaluation of risks to decide if a risk transfer strategy is needed.
- *Perception of need for insurance;* priority setting of things to be insured.
- *Purchasing power;* income and expenditures of the consumer.
- *Evaluation of alternatives to insurance;* the consumer makes an analysis of the insurance service product offered.
- *Evaluation of insurance services;* a price-quality tradeoff is analyzed among the different alternatives the consumer has.
- *Experience with insurance service product;* a satisfaction level together with the desire for renewing the insurance product could appear. This will later affect or "nurture" the consumer's intelligence and insurance culture elements since it adds experience to the person.

Making an analogy between Kahneman's theory and the decision-making process to acquire cyber insurance, the conscious System 2 can be explained with a decision-making model, where analytic and defined tasks indicate the path to be followed to make a decision. The intuitive System 1 can be found in every step of the process since biases and heuristics can always be present when an individual is analyzing a decision. In this context, PMT is useful by providing a way to separate the emotional responses from the cognitive responses.

3.3. Relation of PMT with the insurance decision-making model

This section shows how the two previous sections complement each other, where the PMT model is matched with the insurance purchase decision model and the business process. This is the foundation of the questionnaire for the SMEs. After analyzing the current decision-making models, similarities can be drawn between the elements that play a role in those models and PMT elements. Ulbinaite's model is used to illustrate this due to its broad applicability. Table 3.4 shows the relation between the definitions of both works.

PMT components and elements	Ulbinaite's elements
Sources of information, provide suggestions about possible threats.	
Environmental sources of information, like verbal persuasion and observational learning.	**Influence of communication networks**, local and external interactions.
Intrapersonal sources of information, formed by personality aspects and feedback from prior experience.	
Threat appraisal, a threat must be perceived or identified.	
Severity, the degree of harm from the unhealthy behavior.	**Insurance culture filter**, the how (type of risk) and to which extent (coverage) one's life is already secured. **Family nest filter**, the stage of risk of one's life, e.g., it will be more severe to get health insurance during retirement than when working.
Vulnerability, the probability that one will experience harm.	**Consumer's perceived exposure to risks**, which shows data like statistics of accidents. **Consumer's life quality**, the stage where health status is analyzed. This could be compared with the status of a company's IT security system.
Rewards, determination of the positive aspects for adopting the protective behavior or continuing with the unhealthy behavior.	**Consumer's intelligence (knowledge)**, to determine the possible intrinsic and extrinsic rewards a person has.
Coping appraisal, evaluates the ability to cope with and avert the threatened danger.	
Response efficacy, the belief that the adaptive response will work	**Experience with insurance service product**, if positive experiences have existed, the consumer would have a positive inclination toward using insurance.
Self-efficacy, the perceived ability of the person to carry out the adaptive response	**Consumer's intelligence (Aptitude)**, consumer's risk awareness and sensibility to process and manage financial products, therefore, the ability to carry out the use of the insurance.
Response cost, any costs associated with taking the adaptive coping response	**Purchasing power**, the perception of consumer's affordability to get insurance.

Table 3.4: Comparison of PMT with Ulbinaite's decision-making elements

One thing to notice from the previous table is the repetition of the element "Consumer's intelligence". This repeated use of the element is related to the definition given by Ulbinaite. Since consumer's intelligence is conformed by two aspects, knowledge towards insurance and aptitude toward insurance, it allows for the element to be included in both the Rewards and Self-efficacy PMT elements. After

showing the relation between PMT and Ulibnaite's elements, an adaptation of PMT using Ulbinaite's elements can be done. This is shown in Figure 3.6.

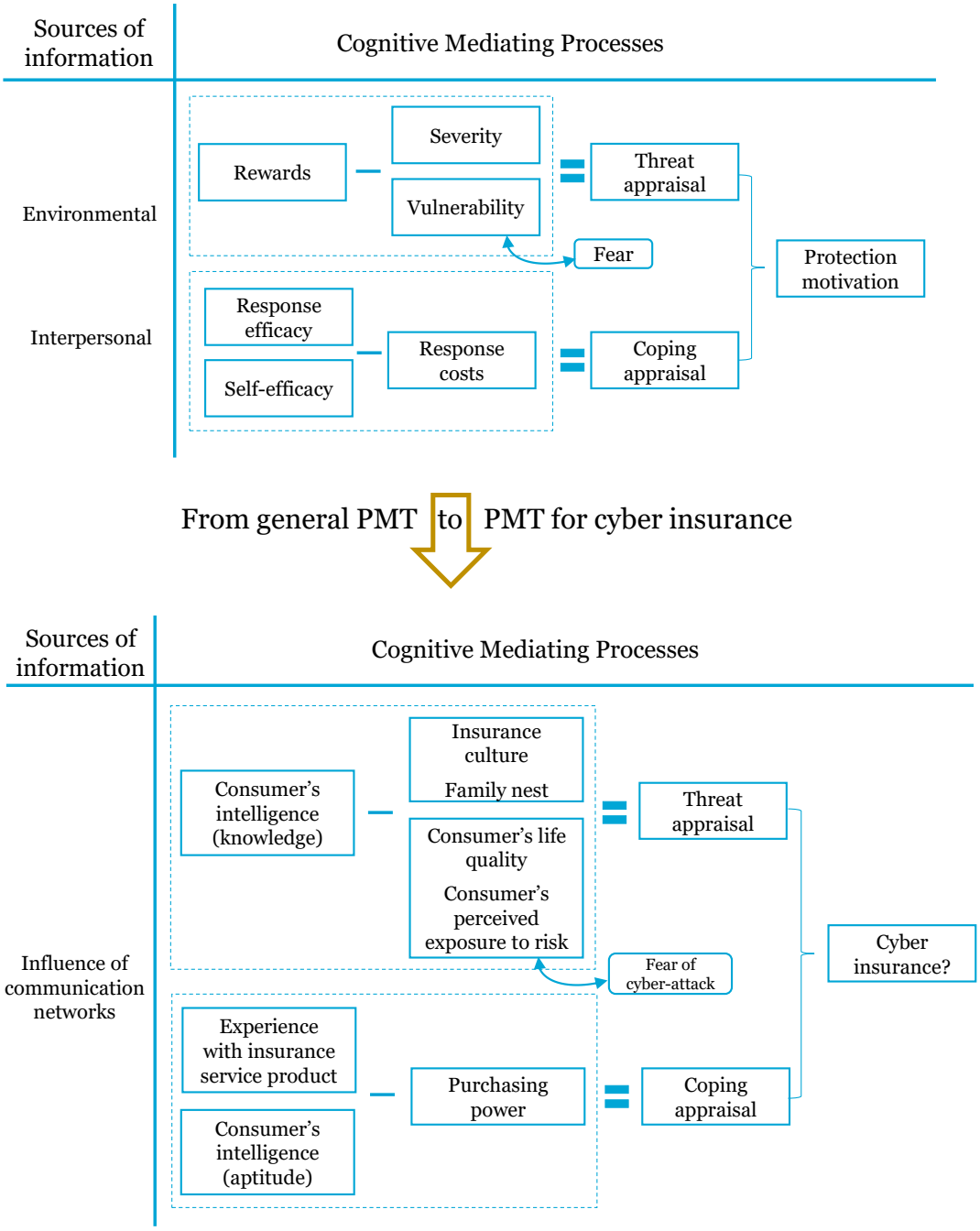


Figure 3.6: Adaptation of Ulbinaite's elements into PMT model

As mentioned before, Ulbinaite's model presented in Figure 3.5 is a condensed version of it. Some steps are omitted to allow an intuitive comparison with the PMT model. The elements included in the original model are omitted here are encompassed in the "Evaluation of insurance services" process. The name of the process is given to the set of steps formed by: perception of affordability for insurance, inclination towards purchasing insurance services, alternatives among insurance service products, price-quality filter, decoy effect, specific insurance service product purchase decision, and insurance service product purchase actions. It is not the intention of this research to explain these

omitted factors, but in general, these steps refer to the evaluation by the consumer of his financial situation, the analysis of distinct insurance products and the consideration of external effects that could impact consumer's choice.

Most importantly, the elements in Ulbinaite's model resemble some of the detailed steps in the business process shown in Figure 3.3. For instance, the Ulbinaite's "inclination towards purchasing insurance services" element can be seen as the step the company takes after the broker has raised awareness about cyber risks. The "alternatives among insurances service products" element can be compared with the selection the company makes after the broker provides different insurance policies. Also, the "insurance service product purchase actions" element represents the decision the company makes after the insurance company provides the final policy offer in the business process. After analyzing the existing decision-making processes for cyber insurance and insurance purchase, three main processes are identified to occur when an SME is analyzing the acquisition of cyber insurance: the cognitive process, the emotional process, and the business process.

3.4. Answers to sub-research questions 1 and 2

The first two sub-research questions can be answered based on the information provided up to this chapter.

SQ1: How does PMT explain a companies' need for cyber insurance? In this research, companies refer to SMEs, and SMEs do not have the specialized personnel in areas like cyber security and risk management unless that is their niche of expertise. Because of this, the decisions made inside an SME can be similar as the decisions made by a single person, and PMT is focused on the way individuals make decisions to protect themselves or not against specific fears. PMT has already been widely used in Information Security and this work is used to explain the different factors an individual could consider to decide whether taking cyber insurance could help protect his company from a cyber attack.

PMT provides the theory for a decision-maker to consider aspects like external experience from other companies suffering a cyber attack or getting cyber insurance and personal experience about cyber security threats. Regarding the threat appraisal process, PMT can help distinguish how severe could a cyber attack be for the company and what are the consequences if the company decides not to have cyber insurance. For the copping appraisal process, PMT identifies what the costs of getting cyber insurance are, and if it could work as promised. As previous research with this theory has shown, PMT can explain irrational decisions in the presence of fear, or rational decisions like analyzing all the costs and benefits of getting protection against a threat.

SQ2: How can PMT be implemented in a decision-making model describing companies adoption of cyber insurance? To answer this sub-research question, two sub-questions need to be answered. For the question ***What is the business process for selecting cyber insurance?***, Figure 3.2.1 describes the process mainly followed in large organizations, where detailed steps and tasks are represented together with the actor in charge to execute them. Then, Figure 3.4 shows the business process for SMEs, where a less developed process is typically followed in this type of organizations. Then, question ***What other factors should be taken into account to define a decision-making model?*** follows the analysis after the business process has been presented because it considers the irrationality that is always presented when individuals make decisions. Insurance consumer behavior research addresses the point that persons do not behave rationally in the presence of risk. Work following this idea is Ulbinaite's (2014), which can help to explain the process a company follows to acquire cyber insurance.

Finally, as has been shown, a business process represents a set of logical steps actors should follow to make a decision, but this process presupposes a rational behavior. Since PMT differentiates the emotional and the cognitive process, it first needs to be demonstrated that a decision-making model includes both types of responses in order for PMT to be applicable. This is done by means of insurance consumer behavior theory, which explains that persons do not behave rationally in the presence of risk and also explains the process for acquiring cyber insurance as shown in Ulbinaite's model. Overall, a decision-making process to get a cyber insurance should involve the cognitive process, the emotional process, and the business process.

The objective of this chapter was to provide enough information to answer the first two sub-research questions. The main outcome is to understand that the research up to this point of the thesis demonstrate that a decision-making model for cyber insurance adoption should include three processes: the cognitive, emotional and business process. The cognitive and emotional processes are identified by PMT and the business process for SMEs is shown in Figure 3.4, which helped to identify the three phases an SME can be when is deciding on cyber insurance. These three processes are fundamental to make the questions in the interviews with SME's representatives.

4

PMT-based interviews

Chapter 4 explains the development of the questionnaire for the interviews with SMEs. First, Section 4.1 introduces the elements the questions should account for, which are gathered from the previous chapter. These elements are related to the cognitive, emotional and business processes. This section also provides the example of questions made for companies that decided to get cyber insurance. Then, Section 4.2 explains the communication process followed with different actors in order to reach SMEs. Also, the process to contact and interview the SMEs is presented. Finally, Section 4.3 introduces the methodology to analyze the data gathered from the interviews.

PMT is a theory that can be applied to research in different ways, the quantitative approach being the most used (e.g., (Reynaud, Aubert, & Nguyen, 2013; Grothmann & Reusswig, 2006; Glenk & Fischer, 2010; Sanner, 1994; Floyd et al., 2000)). Following Section 3.1.1, where the use of PMT components with cyber insurance was presented, in this chapter, the questionnaire is discussed. The work done by Zhang (Zhang et al., 2004) and Posey (Posey et al., 2014) are examples of the use of PMT for qualitative research, which provides guidelines on how to design semi-structured interviews with PMT. The focus here will be on Posey's work since it is applied to the Information Security sector, whereas Zhang's is in the health sector.

4.1. Interview set-up

In the previous chapter, Figure 3.4 showed the three phases an SME could experience when getting cyber insurance. For this study, these three phases are defined as the three scenarios to be used.

I. Company has cyber insurance

II. Company is considering getting cyber insurance

III. Company decided not to get cyber insurance

Since the three scenarios are defined, three different questionnaires are developed. The questionnaires should include questions related to the three processes identified in Chapter 3: the cognitive, emotional, and business process. PMT covers the first two processes. Then, the interview is set-up in the following way:

The general questions collect demographic data about the companies, such as the sector they operate in, company's size regardin the number of employees, the role of the company´s representative and the company´s structure regarding IT security management. Furthermore, general questions also explore the general reasons for the company to acquire (or decline) cyber insurance. Then, business process questions explore the communication companies had with the broker or other actors since cyber insurance was first introduced and how the discussions were handled inside the company. The objective is to identify if the business process developed in Sub-section 3.2.1 follows the same path and which elements are met, which are lacking and if there are elements that should be added.

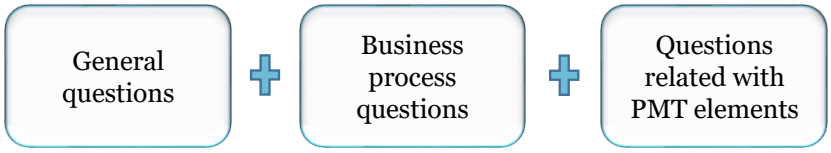


Figure 4.1: Questionnaire set-up for interviews

Finally, the questions related to PMT elements create a match between this theory and the cyber insurance acquisition reasoning. As an example, Tables 4.1, 4.2 and 4.3 show the questions related to each element of PMT. The questions correspond to the first scenario when companies decide to get cyber insurance. The complete questionnaires for this and the other two cases are in Appendix B. As a reminder, the PMT components of Sources of information, Threat appraisal and Coping appraisal, do not have an explicit question since other elements are the ones defining them.

■ **Sources of information elements**

Characteristics to be considered	Question
Intrapersonal sources of information Recognize the individual´s characteristics to identify threats and protective measures. Personality aspects and feedback from prior experience could count for this.	Does your role in the company is related to keeping the company secure from cyber threats? How did you first hear about cyber insurance? Do you know companies who already have cyber insurance?
Environmental sources of information Identify the individual´s external experiences and sources of information that would help him to identify threats and protective measures.	Have you discussed the cyber insurance topic with your clients or other companies? If yes, what was their opinion about cyber insurance? Do you personally know a company that has suffered a cyber attack?

Table 4.1: Questions related to Sources of information component for SMEs that have cyber insurance

■ **Threat appraisal**

Characteristics to be considered	Question
Vulnerability Determine the probability of experiencing harm. Therefore, it can be related to knowing if the company sense a higher or lower probability of being affected by a cyber attack and what reasons influence this probability	What factors make or could make the company more susceptible to security attacks? Meaning, what makes your company easily affected by attackers? Do you have alternative protective measures besides cyber insurance? E.g., IT security measures (firewall, intrusion detection system, antivirus), a business contingency plan or a company's security policy.
Severity Recognize the consequences the company envision if it decides to continue not having cyber insurance and if there are certain threats more damaging than others.	What are the main security threats for which you wanted to get cyber insurance? Do you think some of them have more impact than others?

Continue on next page

Rewards Identify the reasons for which a company would consider that not having cyber insurance has positive aspects.	Is any of the next reasons a potential cause for you to not select cyber insurance? - Do not get cyber insurance until other companies do so. - There are no sanctions for not having cyber insurance. - Do not buy cyber insurance to save budget. - It is not included in the security guidelines of the company. - You think it is not necessary. Can you think of any additional reason?

Table 4.2: Questions related to Threat appraisal component for SMEs that have cyber insurance

■ **Coping appraisal**

Characteristics to be considered	Question
Response efficacy Distinguish if the company believes that having cyber insurance will work and what makes it believe this.	Did the insurer request to implement additional security controls? What are your current expectations with your cyber insurance policy?
Self-efficacy Recognize if the company feels capable of carrying out in a correct way the use of the cyber insurance.	Have you experienced a cyber attack? How did you deal with it? Did you file a claim? Please elaborate. Do you fully understand the coverage provided by your cyber insurance and in which cases you would be able to use it?
Response cost Identify any type of costs the company considers are a consequence of adopting the cyber insurance, these can be financial or social costs.	What potential drawbacks would you associate with adopting cyber insurance? What do you think about the premium price?

Table 4.3: Questions related to Coping appraisal component for SMEs that have cyber insurance

Overall, the questionnaire is made of approximately 20 questions (depending on the scenario). The objective is not to burden the interviewee with too many questions as well as to respect their busy agendas.

4.2. Chasing the data

Wagenaar (2014) indicates that "If you want to learn something new about the topic of choice, there is no alternative but to go out and expose yourself to the world". Wagenaar uses the sentence to introduce the importance of qualitative interviews. Moreover, the quote also goes in line with the objective of using grounded theory since the interviews will provide first-hand data.

The goal of contacting SME's representatives to interview can be simply stated as: reach SMEs in the Netherlands that have dealt with the issue of getting cyber insurance and interview them about it. Nevertheless, experience showed that it cannot be put in a single sentence. The first approach to

get in contact with SMEs is through brokers or insurers. Brokers represent different insurers at the same time, so this seemed to be a more natural path to broaden the possibilities. An alternative to the broker, as shown in Figure 3.2 in Chapter 3 are the Sectorial organizations. The search for both types of actors started in February, and communications with most of them continued until July.

The complete list of actors contacted to have access to SMEs is presented in Table 4.4. By the middle of June, the first six actors in Table 4.4 have been contacted but there were not enough interviews as desired (the objective was to gather between 10 and 20 interviewees with a diversity of companies regarding their status to get cyber insurance). Then, an additional effort was made where A01, A03, and A04 were contacted again resulting in the full list of actors presented in the same Table 4.4. As it can be noted, A05, A06, and A08 could not provide companies' contacts to interview, the reason for A05 was an overload of work while for A06 and A08 was that they do not have direct contact with companies. Finally, for the sectorial organizations A09 and A10, both showed interest but could not provide SMEs contacts. Regarding A11, it was closed due to holiday period and could not be located.

Mark	Actor	Type of activity	Working progress	Starting contact date	Final contact date
A01	Broker	National financial advisor and insurer	Gave feedback on business process and provided contacts about SMEs	13-02-18	11-07-18
A02	Insurer	International insurance company	Provided contact details of brokers	06-03-18	08-05-18
A03	Sectorial organization	National organization for employees	Sent a survey to its members but there was no reply	13-03-18	25-06-18
A04	Sectorial organization	National organization for installation sector	Gave feedback on business process and provided contacts about SMEs	19-04-18	27-06-18
A05	Broker	National insurance company	Gave feedback on the business process but could not provide contacts	26-04-18	04-05-18
A06	Broker of brokers	National insurance broker company	Gave feedback on the business process but could not provide contacts	30-04-18	12-05-18
A07	Incubator	National incubator for technology companies	Provided contacts about SMEs	18-06-18	06-07-18
A08	Governmental advisor	Advisor for digital security.	Could not provide contacts	29-06-18	08-07-18
A09	Sectorial organization	National organization for financial sector	Provided contacts of brokers	25-06-18	16-07-18
A10	Sectorial organization	National organization for transport sector	Could not provide contacts	25-06-18	06-07-18
A11	Sectorial organization	National organization for security sector	Not accessible due to holiday period	25-06-18	12-07-18

Table 4.4: List of actors contacted to have access to SMEs

After all actors in Table 4.4 were contacted a total of 17 SMEs contacts were gathered. Figure 4.2 shows the type of company regarding their cyber insurance process, and their reaction to participating in the interview. As it can be seen, 11 companies agreed to participate in the interview, all of them received the consent form in advance of the interview to know the purpose of the interview and how the data would be used. Of the 6 companies that did not participate, their main reasons are in Figure

4.3.

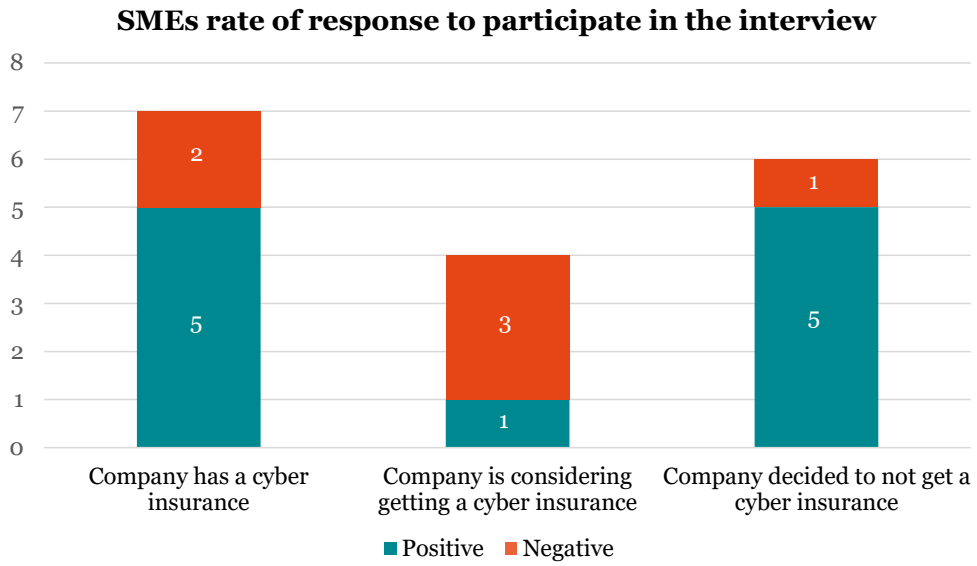


Figure 4.2: Response rate across contacted SMEs

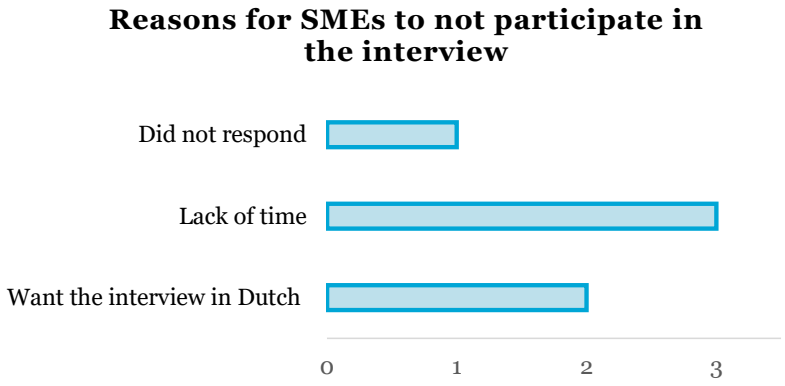


Figure 4.3: Chart identifying the reasons SMEs did not participate in the interview

Regarding the companies that expressed their preference to have the interview in Dutch, as seen in Figure 4.3, it was decided to hold off this option to avoid misinterpretations in the meaning of the questions, their context and the translation from Dutch to English. As mentioned in Section 2.2, the questionnaire was memorized by the interviewer to allow interaction with the interviewee between questions. The potential translator of the interview might not achieve this requisite.

As explained in Chapter 2, after the questionnaire was set-up and committee members provided their feedback, three pilot interviews were arranged before starting the interview process. The main changes after these pilot interviews were related to including an introduction to the topic and the researcher, emphasizing in the academic purpose of the research, and changing the sequence of questions to allow a natural narrative. Once these changes were made, the interview process began. The interviews started formally on May 31st and ended on July 19th. The average duration of the interviews was 35 mins, and except for Amsterdam, each interview was done in a different city.

The reason for making the interview face-to-face instead by phone or virtually was to avoid any technology interruption from the telephone line or the Internet connection. Also, to allow a broader interpretation from the researcher by being able to watch the body language, perceive hesitations and allow explanations not only with words but also with diagrams or hands and facial expressions. These points were endorsed in the following ways:

- Two of the pilot interviews were done by phone due to geographical reasons (the interviewee was in a different country) and in both occasions, problems with the telephone line occurred, because of line interruptions and outside noise.
- In two cases, the interviewees' level of English was not high. Therefore, a switch of words towards the use of hand gestures was done after recognizing hesitation on the meaning from the interviewee.
- In one case, the interviewee preferred to draw a diagram to explain his role at the company and the company's structure.

It must be pointed out that it is not the intention to state that face-to-face meetings are better than distance meetings, the context for the researcher in terms of time and costs is important to consider when deciding to do the interviews in one way or the other. Research has already been done on this topic, and besides time and cost, the objective and field of the research affects the selection to make the interview face-to-face or by phone, or another communication form (Opdenakker, 2006). Thanks to the effective public transport in the Netherlands and the support from the university, the researcher was able to make the interviews face-to-face, combined with the personal interest of the researcher to follow this option. Figure 4.4 shows the cities visited to convene with the interviewees.

Figure 4.4: Cities visited to make interviews to SMEs

SMEs started to be contacted in May after receiving the contact information from the brokers. Figure 4.5 shows the different dates companies were contacted. They are grouped in ”batches”. Each batch represents the point in time when the broker provided the contact information. The timeline in Figure 4.5 shows the constant relation with the brokers to collaborate in the research study, and the continuous talks with the companies to participate in the interviews.

ID	Company	Start	Finish	Duration
1	**1st batch**	**21-5-2018**	**29-6-2018**	**30d**
2	N01	21-5-2018	29-5-2018	7d
3	I03	22-5-2018	29-5-2018	6d
4	I02	25-5-2018	29-5-2018	3d
5	I01	21-5-2018	25-5-2018	5d
6	I05	22-5-2018	29-5-2018	6d
7	N02	21-5-2018	29-6-2018	30d
8	N03	21-5-2018	31-5-2018	9d
9	N04	22-5-2018	14-6-2018	18d
10	I06	21-5-2018	8-6-2018	15d
11	**2nd batch**	**5-6-2018**	**12-6-2018**	**6d**
12	I07	5-6-2018	12-6-2018	6d
13	I04	5-6-2018	6-6-2018	2d
14	**3rd batch**	**14-6-2018**	**22-6-2018**	**7d**
15	I08	14-6-2018	14-6-2018	1d
16	N05	14-6-2018	22-6-2018	7d
17	**4th batch**	**29-6-2018**	**7-8-2018**	**28d**
18	I09	29-6-2018	2-7-2018	2d
19	N06	29-6-2018	12-7-2018	10d
20	I10	17-7-2018	23-7-2018	5d
21	I11	17-7-2018	7-8-2018	16d

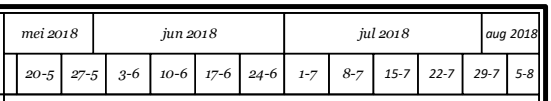


Figure 4.5: SMEs contact timeline

Companies whose mark start with ”I” refer to companies that were interviewed, whereas the ones starting with ”N” refer to companies who declined to participate

Table 4.5 summarizes the interviews by sector, SME type, security management situation, scenario, the lifespan of the cyber insurance (if the company already has one) and if IT services are outsourced or not. An important thing to notice is that I04 is a large company, but it was still decided to keep it as part of the sample. When the brokers were contacted to participate in this study and provide details of SMEs that have been in the process of getting cyber insurance, it was explicitly mentioned that the study is focused on SMEs. Therefore, the requested contacts should also be SMEs. I04 belongs to the first ”batch” and the assumption was that it was an SME. Since all companies were asked about the number of employees working there, at the moment of the interview, the representative indicated

that the company has around 800 employees. The researcher decided to continue with the interview in the standard way and later decide what to do. This topic was brought to the committee, where the number of companies interviewed, the distribution of companies per scenario and the preliminary results were discussed. Two reasons were important in deciding to keep the data from I04. The first one, the sample size was not high, and the second, the distribution of companies per scenario was low for the companies in Scenario III, which is I04's case. If the sample size had increased to over 15 interviews, I04 would have been dismissed, but unfortunately this did not happen.

Company	Sector	SME type[1]	Someone in charge for security management?	Scenario[2]	Lifespan of CI [months]	External IT/ security provider?
I01	Legal services	Small	No	I	18	Yes
I02	Wholesale	Medium	No	I	18	Yes
I03	Financial	Medium	Yes, partially	I	4	Yes
I04	Government	Large	Yes, partially	III	NA	Yes
I05	Financial	Micro	Yes	III	NA	No
I06	Financial	Medium	No	II	NA	Yes
I07	IT	Small	Yes	I	30	No
I08	Installation	Small	No	I	12	Yes
I09	IT	Small	Yes	III	NA	No
I10	IT	Medium	Yes	III	NA	Yes
I11	IT	Medium	Yes	III	NA	Yes

[1] SME size: Micro: 1 - 9 staff headcount; Small: 10 - 49 staff headcount; Medium: 50 - 249 staff headcount (European Commission, n.d.)
[2] Scenario: Refer to Section 4.1

Table 4.5: Demographic data about SMEs interviewed

4.3. Analysis of data

The interviews were recorded and transcribed using Express Scribe Pro v7.01. After transcription, the analysis was assisted using the software Atlas.ti 8 for Windows. Atlas.ti is chosen because of the possibility to assign codes to text lines easily, group codes, create links between them and have easy accessibility to all the documents of the research (i.e., the transcribed interviews). It must be noted that the software helps in performing these tasks, but the qualitative analysis still relies on the researcher.

The first step of the analysis is coding. The main researcher started this after transcribing the interviews and re-reading them. Open coding is the first stage of coding, where non-structure codes are created, meaning that no code is assigned to a "higher range" code, avoiding tree structures. The open coding identifies text segments, as these segments can have one or more codes assigned and each code interprets that statement in a brief word or group of words. For instance, a text segment can be about one of the PMT elements, like vulnerability, where the interviewee is explaining the main security threats they are concerned about, and by doing this, he also gives examples of frequent cyber attacks. In this case, the code for the PMT element is assigned, and odes for the type of attacks that were mentioned.

For example, Figure 4.6 is the screenshot of the open coding process for an interview's segment. In this example, the researcher is asking the interviewee "What factors make or could make the company susceptible to security attacks?", this is a question corresponding to the vulnerability PMT element. In the response, the interviewee explains the company has legacy systems (the vulnerability factor), which from a technical point of view makes them susceptible. Nevertheless, the company has never been hacked, which is assigned to the self-efficacy's PMT element with another code. The interviewee continues explaining that because they are a small company, they lack specialists in IT security. This sentence is coded as "Risk: Attacker motivation". Finally, due to this vulnerability the company has, an attacker could try to commit financial fraud, coded as "Threat: Financial fraud". More codes were assigned to this segment of the interview, but the ones mentioned illustrate the process of open coding.

After the open coding is done for all the interviews, the external supervisor performed a control review to identify if there are important aspects from the interviews that were left out. The two coders met to review the generated codes and agreed on the selection of group codes, which are based on relevant themes related with answering the sub-research questions. Example of these themes

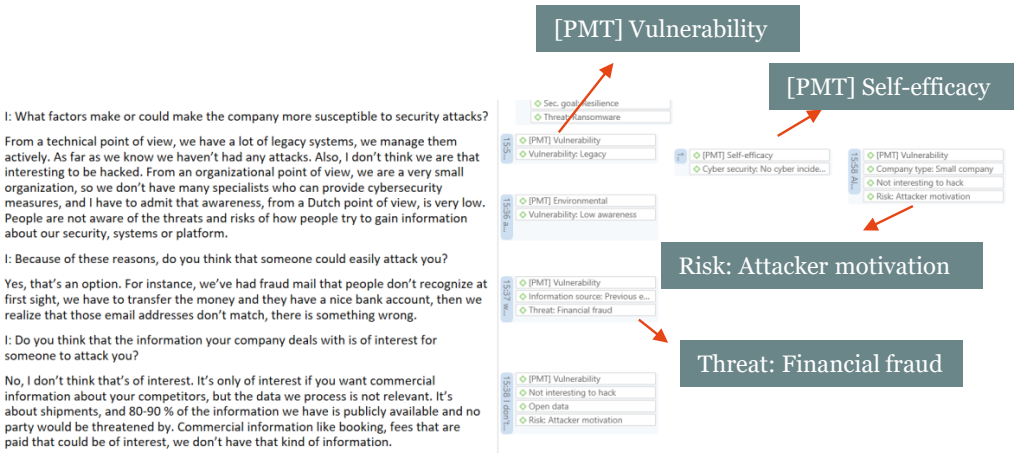


Figure 4.6: Example of open coding process in Atlas.ti

are companies' experience with cyber attacks, cyber security knowledge, cyber insurance knowledge, security threats, opinion about the business process, security controls in place, insurance policy, and other. It is important to notice that not all the codes need to be grouped.

By the time the open coding process finished, a total of 161 codes were identified. Afterwards, an iterative process was followed to make a "cleansing" of the codes by grouping or deleting them, with the goal to form categories, meaning groups of codes. This cleansing process resulted in a total of 16 code groups. Groups are formed by aggregating similar categories. For instance, anything related with the business process goes to the "CI process" code group, which contains codes such as negotiation with managers, research, responsible for security, additional information requested, and other codes. Another example is for security threats. The code group "Threat" is made up of codes like phishing, ransomware, data leakage, financial fraud, cyber criminals, and others. Appendix C shows the full list of codes and their corresponding groups. Figure 4.7 illustrates in a simple way the coding procedure for every interview.

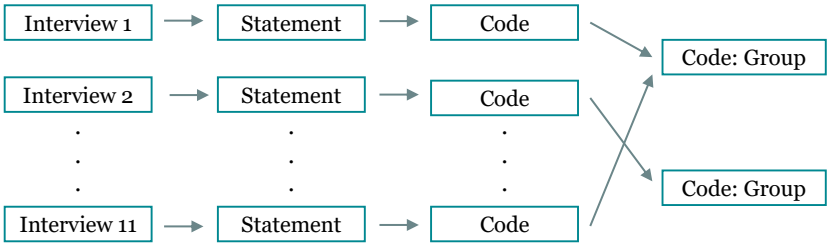


Figure 4.7: Data analysis procedure in Atlas.ti

Like any methodology, advantages and disadvantages exist. Semi-structured interviews are a useful way to gather data from primary sources and is commonly used when a topic has not been widely documented. This is the case for cyber insurance adoption. Nevertheless, since the topic is still novel, there are not many companies that have been through the process of acquiring cyber insurance, or they are reluctant to talk about it. In this chapter, it was explained how the questionnaire was developed based on the PMT definition, where specific questions were adapted to each PMT element. Then, the process to contact the SMEs to interview them is explained. In the end, 11 companies agreed to participate. Even though the number is lower than the initial intention, each interview provided useful insights regarding the decision process they followed to decide whether or not to get cyber insurance. Finally, Atlas.ti is the software used to assist with the qualitative analysis. The open coding and group coding process are explained in Section 4.3. This analysis guided towards the results exposed in the next chapter.

5

Results

Chapter 5 brings together the qualitative analysis collected from the interviews. Section 5.1 is formed by three sub-sections corresponding to PMT's sources of information in Sub-section 5.1.1, and the two PMT processes, threat appraisal in Sub-section 5.1.2 and coping appraisal in Sub-section 5.1.3. The PMT section contains the greater amount of information of this chapter since PMT is the backbone of the questionnaire made to the SMEs. Section 5.2 shows the findings for the business process. The results for topics not corresponding to the PMT or business process are in Section 5.3. These results emerged throughout the interviews appearing to be important regarding cyber insurance adoption. Finally, after all the previous analysis is done, drivers and impediments for cyber insurance adoption are distinguished in Section 5.4.

5.1. Results for PMT

The results generated from the analysis of the transcribed interviews through the use of semi-grounded techniques are shown per PMT component. As a reminder, the questionnaire was elaborated to cover the three different scenarios detected during the business process to acquire cyber insurance. Nevertheless, the interviews held for this research gave a total of 11 interviews with the distribution shown in Table 5.1. As it can be seen, the proportion is significantly different for the companies in Scenario II due to the low rate of positive response. Then, the comparison of answers can only be done between companies in Scenarios I and III. Moreover, this is supported by the fact that the company in Scenario II, expressed at the time of the interview recently decided to get cyber insurance.

Number of SMEs interviewed. per scenario	
I. Company has cyber insurance	5
II. Company is considering getting cyber insurance	1
III. Company decided not to get cyber insurance	5

Table 5.1: Distribution of SMEs interviewed

5.1.1. Sources of information

In other words, how did you first hear about cyber insurance? Do you personally know a company that has suffered a cyber attack? (No, news in the media does not count)

This is the only PMT component for which the same questions were made to all the companies regardless the scenario they belong to. Since PMT is focused on individual's behavior, **sources of information** is the only element not focused solely on the individual but on the type of information surrounded by. Due to this, the questions are not guided by the type of scenario the company is in.

Regarding the ***intrapersonal*** element that deals with personality aspects and feedback from prior experience. Four representatives indicated to have knowledge about the existence of cyber insurance.

From these four affirmative answers, three correspond to companies deciding not to get cyber insurance. Interestingly, two of the answers correspond to finding about cyber insurance through their personal experience:

> *Because of the news, magazines, internet forum, you read a lot about it. At the moment the broker came I knew about it.* ***(I02)***
> *I'm aware from reading the press, I know it exists.* ***(I10)***

Whereas the other two interviewees discovered cyber insurance as a solution surged from their business activities:

> *We thought of it as selling our product to insurers to reduce the risk. We read about it and we talked about the opportunity that could be there for selling our product.* ***(I09)***
> *It was a long time ago. There were two big banks that started to research how to provide coverage for cyber incidents, and our company was one of the first to provide them with the information they need.* ***(I11)***

When interviews were requested, it was requested that the representative should be involved in the process for selecting the cyber insurance. From the representatives interviewed, 9 out of 11 have a degree of responsibility for keeping the company safe of cyber threats, but all of them had a role on the decision-making process. The two representatives that do not have this specific role in the company oversee areas related to risk management. Then, it is true that their role is not directly related with "keeping the company safe from cyber threats", but they do participate in the process of deciding how serious a threat like this could be.

Only two companies know of other companies with cyber insurance. In both cases, their professional network provided this knowledge and the possibility to discuss it with their fellow companies; only one of them decided to discuss the topic. Through this question, it was found that the Nederlandse orde van Advocaten[1], through its local bars, makes the recommendation to its members to get cyber insurance. Because of this, law firms belonging to the same local bar know that some of the members have cyber insurance. Nevertheless, even that they belong to the same network, the interviewee said he did not discuss the topic with others. This aspect of discussing a topic with an external party and the next feature is related to the ***environmental*** element.

When asking if they knew companies that had suffered a cyber attack, a common answer was yes, but after being emphatic that the question is referred to personally knowing the affected company than hearing or reading about it in the news, the answer was adjusted. It is interesting to make a differentiation between the answers provided by 5 of the 11 companies that responded affirmatively:

- I02 knows about clients that suffered a ransomware attack through email.
- I06 met companies that suffered a cyber attack after the broker took them to presentations where companies shared their cases.
- I07 knows other companies due to an external group he belongs to, this is not part of his direct job responsibilities but he considers as a useful extension of it.
- I09 and I11 business activities are related to providing cyber security tools

I02 is the only company knowing about cyber attack victims through their own sources of information, in comparison with I07, I09, and I11, for whom professional activities lead them to have direct contact with companies being the target of cyber attacks. In other words, for I07, I09 and I11 this knowledge is strictly related to their activities, whereas for I02 is more related to a coincidence.

[1]The Netherlands Bar in English, for more information visit: https://www.advocatenorde.nl/

5.1.2. Threat appraisal

Or, how vulnerable to cyber attacks do you think you are? What are your biggest cyber fears? And, what are the reasons for not getting cyber insurance?

According to PMT, the first process to start is **threat appraisal**. One of the advantages of using Atlas.ti software is the promptitude to analyze different themes from the documents after the codes have been identified. In this sense, after identifying the factors for ***vulnerability*** element, it is possible to get a quick view of the type of answers given and the most used words. A quick snapshot is in Figure 5.1, where a larger font size of the word indicates that it was mentioned more often. After the software gives a start about where to look, the researcher can navigate through the documents more easily and analyze the given answers.

Figure 5.1: Snapshot of Atlas.ti to visualize quotations related with a code and its most used words

As it can be seen from Figure 5.1, the repetition of words like data, cloud, cyber, digital and information, can be grouped in a factor that can cause a company to feel vulnerable, *digitalization*. Below are some answers illustrating this observation:

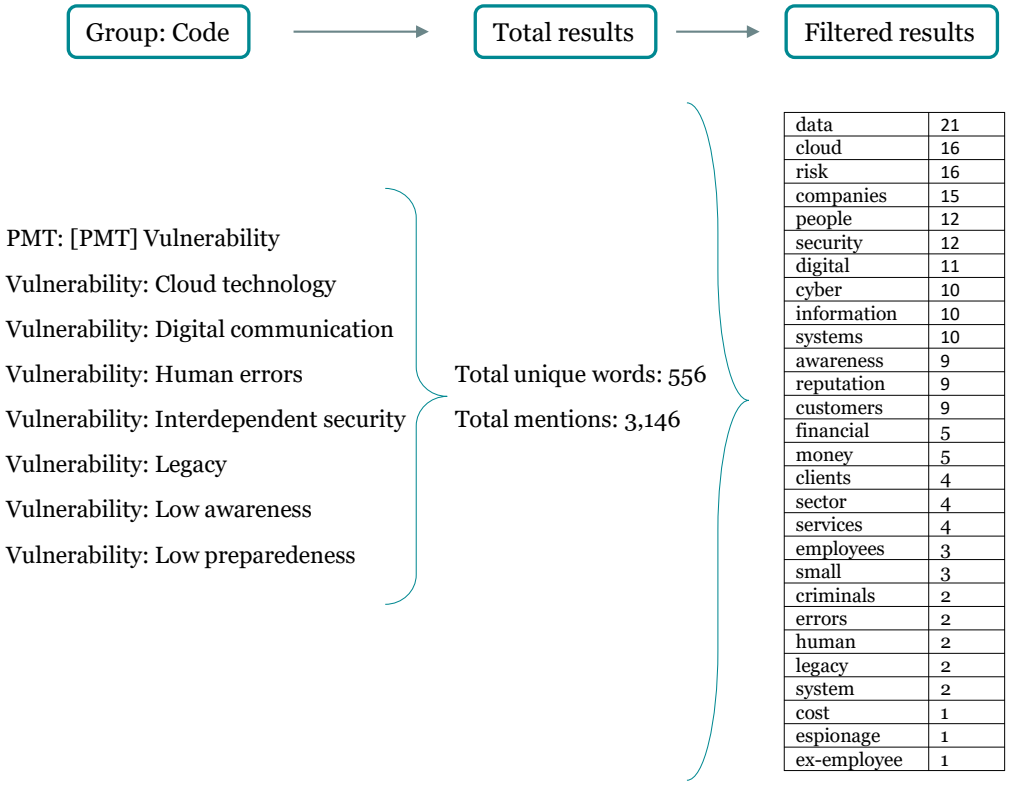
> *We have our data in the cloud, so that makes us much more vulnerable. Although our IT company says it is better protected than the paper trail, I don't know but that makes us more vulnerable.* ***(I01)***
> *The threat is from the outside that is looking for an entrance opportunity, a weak spot. That can come from all over the world because we are in the cloud, we are very dependent on our supplier.* ***(I03)***
> *When we have our own IT system in place, SAS solutions in the cloud, you have to deal with that risk.* ***(I06)***

Depending on the company's activity, *digitalization* can be related to the threat of losing *confidential information*, especially client' information companies need to store. Another factor commonly cited is *reputation*, SMEs highly value their reputation. They believe attacks can occur to damage their reputation, but they also believe reputation is something that needs to be protected. Then, reputation acts as a trigger to seek protection.

The rest of the reasons mentioned, but less frequently than *digitalization*, *confidential information*, and *reputation* are listed next. These factors cannot be directly obtained from the snapshot in Figure 5.1 because it depends on how many times a word was mentioned. Therefore, an overview of how the answers were extracted is showed in Figure 5.2. The listed reasons were identified following an analysis from the answers provided by the interviewees after the question, "What factors make the company more susceptible to security attacks?" was asked. As it has been mentioned, the software guides the researcher, but the final analysis is done separately. In this case, if an answer like "espionage" was mentioned once compared to 21 times the word "data" did, it does not mean that a unique result should

be dismissed. The number of interviews gives the opportunity to analyze each answer individually and determine a relative value to the answers instead of an absolute one.

- Security interdependency
- Money
- IT and security services
- Legacy systems
- Human errors
- Espionage
- Criminals (national and international)
- Lack of specialists
- Disgruntled ex-employee
- Lack of awareness
- Being part of the financial sector
- Customers with high revenue



data	21
cloud	16
risk	16
companies	15
people	12
security	12
digital	11
cyber	10
information	10
systems	10
awareness	9
reputation	9
customers	9
financial	5
money	5
clients	4
sector	4
services	4
employees	3
small	3
criminals	2
errors	2
human	2
legacy	2
system	2
cost	1
espionage	1
ex-employee	1

Figure 5.2: Codes generated for the answers related to the Vulnerability element

Next, more information is provided for some of the factors listed above. Similar to *reputation*, *lack of awareness* is seen as a potential reason to be attacked but also as a consequence to get cyber insurance. A contradiction in opinion between companies is related to IT and security management services. Some companies consider it best to have the control of this service, while others prefer to leave this in the hands of specialized companies. The relation of companies with outsourced services can be seen in Table 4.5. To illustrate this point, I06 and I11 expressed their wish to depend less on their external provider in the near future, whereas I07 indicated they prefer to manage IT systems by themselves, but at the same time recognized that taking this responsibility implies a vulnerability. Some of the statements made regarding the reasons previously listed are:

> Security interdependency. *Another risk is that you have contact with your clients, and possible dangers can come from your clients that will be incorporated into your systems.* ***(I03)***

> Money. *We deal with public money, that makes an extra point for the reason we wanted to buy the cyber policy.* ***(I06)***
> Lack of specialists. *We are a very small organization, we don't have many specialists who can provide security measures.* ***(I07)***
> Espionage. *We are protecting against anyone who wants to influence our software that operates in the national government, this would be espionage related.* ***(I11)***

Finally, I06 did mention that just the fact they belong to the financial sector makes them vulnerable. It is not a coincidence that the second most popular sector to be interviewed belongs to the financial sector. The recent Ponemon Institute study (Ponemon Institute, 2017) indicates that the financial sector is the one with the highest costs of cyber crime by industry sector.

Moving to the next threat appraisal element comes ***severity***. The questions to analyze this element try to find out if companies know how they could be attacked and the consequences of it, which would be linked with the answers provided before for the vulnerability element. The main identified security threats are *data leakage*, *service disruption*, *phishing*, and *ransomware*. The threats were coded to identify them easily, next the threats were grouped. In total, this code had a total of 77 grounded codes. The four threats showed in Table 5.2 represent the threats that were mentioned by more than three companies. This is important to mention because one threat could have a grounded number of 6, but it is only linked to one company. The latter means that the interviewee mentioned the threat several times.

Threat	Grounded
Threat: Data leakage	12
Threat: Service disruption	9
Threat: Phishing	8
Threat: Ransomware	7

Table 5.2: Threats identified from the interviews and number of times they were mentioned

Some of the statements made regarding these threats are:

> *If companies have had attacks is in cases when an employee clicks in the wrong link, almost every company has had that experience.* ***(I01)***
> *We have millions of contractors and with that data you could know where they live, the email addresses, bank accounts, all that kind of information. If they come to them is no good.* ***(I04)***
> *We are especially aware of hacks of data. We have to have a reputation plan in case it happens.* ***(I05)***
> *We have had fraud mail that people don't recognize at first sight, we had to transfer the money and then we realize that those email addresses don't match.* ***(I07)***

In general, the most significant security threats companies want to be protected for are related to keeping their data safe from leaks, avoid service disruption and be protected against threats they have not yet considered. The latter point is caused by the fact the companies are not experts in cyber security topics, one of them indicating they choose cyber insurance *"just in case"*.

Even if companies have cyber insurance, protective measures should be in place since the combination of both is considered ideal to mitigate cyber risks. Another question to analyze the element of severity was about protective measures the company has implemented. In most of the cases, examples had to be provided by the researcher, like antivirus, firewall, business contingency plan and others. Next is provided a recap of the answers provided in the 11 interviews:

- In three cases, giving examples did not result in the interviewee expanding more on the answer.
- For one case, examples were not provided but the only answer given was, "firewall".
- In two cases, respondents indicated that they pretty much lack of any IT protective measure.

- For the rest of the five cases, the respondents did elaborate on their answers. These answers are broken down as follows:
  - 4 out of 5 cases correspond to the total sample of companies in the IT sector.
  - 4 out of 5 cases correspond to companies in Scenario III, they decided not to have cyber insurance. 3 out of these 4 companies are from the IT sector.
  - One of the representatives included awareness as part of the protective measures.
  - Two representatives indicated they include lawyers among their protective measures.
  - One of the companies do social monitoring as part of their security measures.

Regarding the last point, for the companies in Scenario III, it was visible during the interviews the high degree of care the companies have for preventive measures. Some of the measures that were mentioned are back-ups, internal procedures for data access, installation of an additional data center, encryption of communication channels, intrusion detection systems, and collaborating with experts in not only IT but also the legal field.

Finally, the ***rewards*** element to assess the Threat appraisal process according to PMT theory indicates that there are reasons the individual finds it attractive to continue with the "unhealthy" behavior. The three main reasons companies mention not to acquire a cyber insurance are *price*, *not necessary*, and *unclear policy*. Some of the answers given regarding these reasons are:

> *When the broker started with the offer, the premium was much more higher than it is now, at that point was one of the reasons to not get cyber insurance.* ***(I01)***
> *The platform has been up and running for 20 years, and in those 20 years we haven't had any incident. So, there were no actual reasons for having it (the cyber insurance).* ***(I07)***
> *If it cost too much (the cyber insurance), we wouldn't have get it.* ***(I08)***
> *Having had the experience with insurance like car or house insurance, knowing how difficult is to make a claim, I couldn't begin to imagine how this would look in a complex situation with a cyber insurance claim. I have low confidence that a claim would be successful.* ***(I10)***
> *They simply can't cover certain things. They would not understand what we need, or we wouldn't trust them. Not all insurers are cyber-aware enough, or the sales people aren't.* ***(I11)***

A couple of additional reasons were mentioned by companies with cyber insurance. Two representatives mentioned that bringing a clear analysis to the final decision-makers in the company was not an easy task, making a *cost vs benefit analysis* an additional reason for the rewards element. The other reason is the existing *interdependence* of risks, as one company indicated that they are managing the risk on their own since other companies do not have to take the cyber insurance like they decided to do it. On the other side, other companies had a different opinion:

> *When we think is good for a company we do it and we don't care what the others do.* ***(I01)***
> *It's kind of similar to the car insurance, it depends on the driver.* ***(I02)***

From the literature review it was assumed that the process to get cyber insurance could be complicated. Nevertheless, it seems that brokers have done a good job helping their clients to follow an easy process because otherwise, they would have opted for not getting the cyber insurance, as stated by the interviewees in two occasions.

For the companies that decided not to have a cyber insurance, additional reasons that were mentioned are *preventive actions*, *uninsurable risks*, and *no added value*. Some of the statements made by the companies are:

> *We are quite secure because we have good security engineers working at our company. So, by putting the same amount of effort in technical measures we cover it*

better than with the insurance. The biggest risk for us is to be out of business after a breach ***(I09)***
For us, reputation is the most important and insurance doesn't help with reputation, that's why we didn't take any insurance. ***(I05)***
We don't need the insurance, we know what to do if something happens and who would help us. ***(I04)***

A resume of the reasons being part of the rewards element is provided in Table 5.3 together with a short description of the reasons to avoid misunderstanding on the meaning.

Reason	Description
Price	When the premium price is considered to be high.
Not necessary	Related to the low probability of occurrence of an attack.
Unclear policy	The policy is not clear regarding the coverage, the cases when a claim is applicable, and the risks calculation.
Cost vs. benefit analysis	Translating the insurance benefits in a concise and clear way for managers.
Interdependence	Sharing of risks with other companies.
Preventive actions	Security measures in place surpassing the ones provided by the insurance.
Uninsurable risks	Risks perceived by a company that cannot be covered by an insurance.
No added value	When a company has considered diverse ways to protect against cyber attacks and believes the insurance cannot provide anything additional.

Table 5.3: Reasons corresponding the PMT rewards element and their corresponding description

5.1.3. Coping appraisal

Putting it differently, are your security controls enough? How confident are you with your own capacities? Money is important but how much?

The PMT process that evaluates the ability to cope with and avert the threatened danger is **coping appraisal**. The three elements defining the coping appraisal component are response efficacy, self-efficacy, and response costs. Since coping appraisal implies selecting an option to cope with the threat, the questions made to companies vary depending on their scenario.

For ***response efficacy*** element, if the company is in Scenario I the researcher asked if the insurer required to implement additional security controls in order to be insured. Whereas if the company is in Scenario III, the focus is to know if the company believes that their security controls in place are enough to deal with cyber risks. Moreover, for companies in Scenarios I and II, asking about their expectations about the cyber insurance would help to identify if by adopting this measure they felt able to deal with the risks.

Regarding the security controls requested by the insurer, no company was asked to implement additional security controls to get the cyber insurance. However, there were differences in the responses given, even for companies working with the same broker. For instance, I01 stated the following:

Part of the insurance is a check by two companies and we still have to make the appointment, but that's part of the offer. ***(I01)***

However, other companies indicated that no previous check was done. One interviewee first indicated that controls like screen lock, use of private network and a two-factor verification for remote access was requested, but further, it was asked to elaborate on the answer:

> *They didn't have real hard requirements. I use their requirements and advice to bring the awareness to the company.* ***(I03)***

For the companies that decided not to have cyber insurance, one of them just mentioned they should work more closely with fellow companies to help each other. The other four were emphatic in the protective measures they have in place. When asked about additional security controls, only three of them elaborated on the answer, the other one indicated that it is a question for the ICT department and not for him. The answers provided are:

> *Right now no, we are implementing all the controls.* ***(I09)***
> *Every company could always do more. Then it comes to a balance where it's cost effective. We have project ongoing, which will continue to improve our security. Is not something that you do and then stops.* ***(I10)***
> *Be more proactive. Specifically looking for potential attackers on the network.* ***(I11)***

Another example about the use of the qualitative software is when the expectations of companies about cyber insurance were explored, for companies in Scenario I. After finishing the coding, it is easier to access the answers provided depending on the assigned code. Figure 5.3 shows, in a nutshell, the answers related to this topic. Six companies gave their answers, generating 13 statements. Some of the statements are repeated. After grouping them, nine types of unique answers were identified. The answers are finally divided in five classes as shown below.

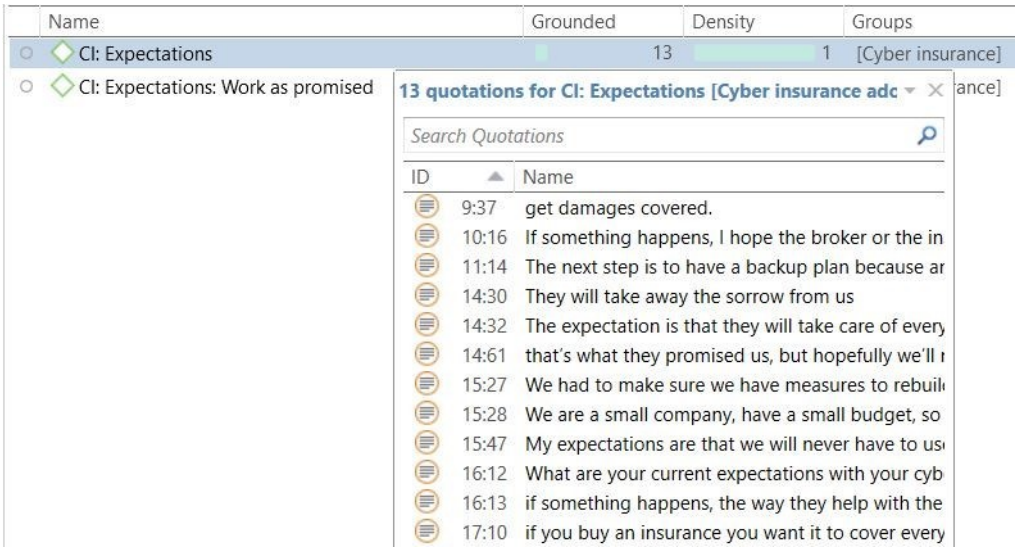


Figure 5.3: SMEs expectations on cyber insurance

- 3 out of 9 answers are related to getting appropriate help during the process in case of an attack.
- 2 companies expect they will not have to use the insurance.
- 2 answers are related to implementing the policy as established.
- 1 company refers to the advantage of having a 24/7 assistance.
- The final answer provided by one company is "take away the sorrow from us".

For the next element, ***self-efficacy***, there is a similar question made for all the companies, to know how they dealt with a cyber attack in case it has occurred to them. Three companies indicated they suffered a cyber attack. Two of them correspond to companies in the Scenario I, and both cases happened previous to getting the cyber insurance. In one case, the representative did not yet work there so he could not give additional insight into the process. In the other case, the representative

mentioned that the data leak was caused by a phishing email that cost half a day of inactivity. The third company suffering a cyber attack is in Scenario III. The representative provided details about the type of attacks occurred and how they dealt with them. This company proved to be an exceptional case compared to the rest of the interviews. Even though attackers have successfully penetrated their systems, the damage caused is not considered to be substantial. Moreover, the way they implemented their security tools has shown them that even they are vulnerable of being attacked, yet the company can control the damages, something they do not see to be provided by insurance. A point to clarify regarding this company is that their business activities are related to providing cyber security tools, then, their case cannot be extended to any SME.

The rest of the analysis for the element self-efficacy is split depending on the companies' scenario. Regarding companies in Scenario I, the objective is to recognize if they feel capable of carrying out the use of the cyber insurance by asking them about their level of understanding of the policy, the coverage, and the cases when the policy is applicable. All the companies in this scenario indicated that the cyber insurance policy is understandable and clear.

For companies in Scenario III, the self-efficacy element should be assessed based on their IT security management currently in place. One company's representative indicated that current security measures are enough. The other four companies in Scenario III said they do believe to have a good security management strategy. Following this, it was asked if there were reasons that would motivate companies to buy cyber insurance, the answers were:

> *What we need is someone to talk to the press, but that's already in our business contingency plan. That's why we don't need the insurance.* ***(I04)***
> *I don't see any reason. Reputation risk can't be insured.* ***(I05)***
> *I can't think of any reason.* ***(I09)***
> *If we found that we have been compromised, that would make us think that our security needs to be stronger. In the meantime, we need to cover ourselves until we show we have worked on this. This is one scenario. The more likely scenario is customer pressure, then we would act to get insurance for this.* ***(I10)***

The last element, ***response cost*** is naturally related to the premium price, especially since literature indicate that cyber insurance prices are high, and this could be a reason for companies not to get one. Nevertheless, one answer is backing up this notion. Figure 5.4 indicates the rate of responses, where "Don't know" belongs to four of the companies in Scenario III, for which the question was asked but they said they did not get in that point of the negotiation.

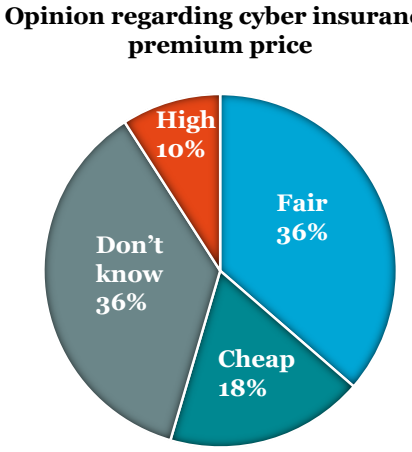


Figure 5.4: Responses regarding the premium price of the cyber insurance policy

Finally, for companies in Scenario I, their decision whether to renew the insurance and to assess the success of having it, none of them have long-term expectations. Everyone indicated that predictions could not be made until something happens but at the same time, none of them have any reason

to terminate the insurance. However, one company did mention they would consider changing it if a better offer appears.

5.2. Results for business process

That is to say, how are decisions made in your company? (And yes, we are almost done with the interview)

The questions regarding the process SMEs followed with the broker had the aim to know general aspects about it and identify any problems the SMEs had during the process. Also, this would help to realize if the SMEs' process has similarities with the process showed in Sub-section 3.2.1. As explained in this section, after the interviews with brokers it was found this actor has a proactive role in creating awareness about cyber insurance. From the interviews with companies in Scenario I, in all of the cases, the broker was the first one who approached the SME to discuss the cyber insurance product. Besides, except for one case, the interviewees had no previous knowledge about the existence of cyber insurance before the broker approached them. Moreover, regarding the company that did have previous knowledge about cyber insurance, he expressed "the broker's representative is a very good salesman", giving an emphasis that the broker's representative helped in giving more confidence about the product.

Secondly, an internal decision-making process was detected in the first interviews and confirmed throughout the rest of the interviews. The broker will first approach a company's representative, who often is not a director or part of the board. Then this person will take the offer to the final decision-maker of the SME, and this step could be taken personally or together with a team, depending on the structure and number of personnel. Afterward, the decision is taken by the director. Overall, the process is straightforward and could take from 3 days to 1 week. During two interviews, the process took longer because the person approached by the broker was convinced, or partially convinced, on the advantages of having the insurance but not the final decision-makers, one company described it a "the decision-making process was quite intensive".

In the previous paragraph, it was mentioned that the decision to take the cyber insurance offer to the final decision maker could depend on one person or a team. This stage depends on if the person has or does not have knowledge about information security, where the next phases can be seen:

- If the person considers having enough knowledge about cyber threats and security protective measures and does not have to report the decision with more members of the team, he will make the decision to take the offer to the next stage.
- If the person believes to have enough knowledge about cyber threats and security protective measures but does have to report the decision with colleagues, he will first consult with the team.
- If the person does not have enough knowledge about cyber threats and security protective measures, he will make a consultation with the IT department (either internal or the outsourced party).

An additional result that emerged when the process to get cyber insurance was discussed is the similarity some representatives thought it exists between cyber insurance and other types of insurances (also called "silent coverage" (OECD, 2017)). This silent coverage was valid for three companies, who mentioned that liability insurance was thought to cover damages similar to the ones cyber insurance does.

> *Two years ago they mentioned cyber insurance, at that point we didn't think it was really necessary and we also thought it was already covered by our professional liability insurance, but that was not the case.* ***(I01)***
> *We have several brokers because we have different insurances. I compared this broker with another broker we use for other liabilities because we also have a big insurance for professional liability. -Interviewer: Did you think that the professional liability would include the cyber insurance?- Yes, I discussed that because that was one of the questions I had. Is this something that is extra or is not included in other liabilities?* ***(I03)***

> *We had an insurance when I started working here but it was like an economic insurance, for liability. But the cyber insurance is current because of the ways the platform behaves with our customers.* ***(I07)***

As it can be noticed, two companies explicitly believed the professional liability insurance had the same coverage as the cyber insurance, whereas the third company could see the difference and therefore decided to get the cyber insurance to have the coverage needed.

5.3. Other results

Part of the objective of getting data from semi-structured interviews and using semi-grounded theory is to discover results not envisioned. This happened to be the case for topics beyond PMT influencing companies to make a decision regarding cyber insurance. The three topics identified throughout the interviews are:

- ***Cyber insurance market***. The cyber insurance market for SMEs is small, and companies acknowledge this. Two companies indicated they tried to look for additional options than the first presented by the broker. Their research showed that there were no more than two or three additional options. Trust in the broker plays an important role for SMEs since they can trust the advice given to them without having to spend time looking for alternative options. One company even mentioned that all the insurances are with the same broker, including now cyber insurance; this is useful for them since the point of contact is only one person. Additionally, one of the companies that decided not to have cyber insurance mentioned that "in 5 years, cyber insurance will be as normal as liability insurance", which shows the growing tendency perceived by some companies regarding cyber insurance.

- ***Cyber insurance validity*** Cyber insurance proved to be a new product where the company that has had the product for longer corresponds to a period of 2.5 years. The question about the validity period for companies in Scenario I was not considered when the questionnaire was developed, but it naturally appeared since the first interview. Then, it was decided to incorporate it into the questionnaire. Figure 5.5 shows the validity time for the rest of the companies that decided to have cyber insurance.

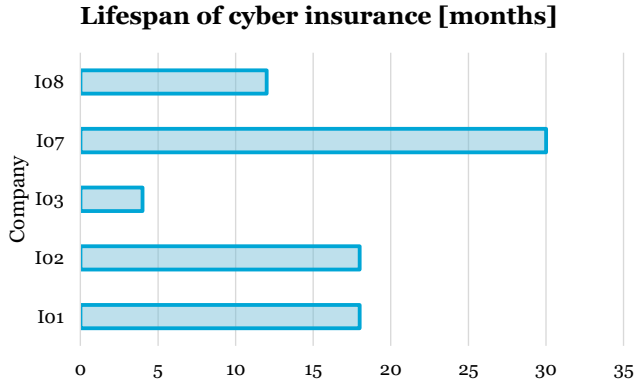


Figure 5.5: Lifespan of cyber insurance for companies owning the product

- ***Moral hazard*** Moral hazard occurs when the insured takes more risks than it would if the purchase of the insurance had not occurred. When the PMT element response cost was analyzed for companies in Scenario I, there is a question about the drawbacks associated with having cyber insurance. It must be remembered that the response cost element does not only involve financial costs but also includes any negative cost associated with getting cyber insurance. When the question about potential drawbacks was made, only one company mentioned:

> *Now that we have insurance we could be less aware or think that everything is taken care.* ***(I03)***

However, they then discarded that possibility since the company is creating a plan not to allow that to happen. This potential drawback was mentioned in more interviews, but companies always indicated that they did not see something like that happening. However, for the company cited (I03), the option was not mentioned, the representative brought the topic as a potential drawback for having cyber insurance.

5.4. Approaching or deviating from cyber insurance

SMEs are in constant struggle for creating a name so they can persevere in the market. They know it is not possible to have experienced personnel from different sectors working at the company, and because of this, they are focused on delivering a product or service in the most cost-efficient way. During this research, questions related to PMT elements and business process were made in order to understand their reasons for choosing or not to have cyber insurance. The objective of making these questions was also to find through the interviews the primary drivers and impediments for Dutch SMEs to get cyber insurance.

It is important to distinguish the difference between making specific questions like, ”Why did you get cyber insurance?” or, ”Why did you not get cyber insurance?” and finding these answers through the reasons that guide people to execute certain actions. For this research, the second approach was chosen. Then, by analyzing the answers provided about PMT and the business process, the drivers and impediments are detected along the way. The followed steps started by looking at the generated codes and choose the codes with a higher grounded number [2] that are related either to drivers or impediments for cyber insurance adoption. The codes chosen for each case are shown in Table 5.4.

Driver	Grounded	Impediments	Grounded
Asset: Company’s reputation	21	[PMT] Rewards	39
CI adoption: Driver	52	CI adoption: Impediments	25
CI process: Business contract	37	Risk: Perceived exposure to risks	26
Cyber security: Knowledge	16		
Premiums: Price	26		
Sec. goal: Awareness	28		

Table 5.4: Codes selected to analyze drivers and impediments for cyber insurance adoption

The selection of the codes is based on what has been learned so far about the reasoning companies have regarding cyber insurance. After defining the codes, a report and a list of most used words were created using Atlas.ti. Both reports generated a bit more than 35 pages, and the counting of words cannot eliminate words like articles or nouns. As a reminder, Appendix C contains all the codes generated for the 11 interviews. To provide a visual example, manual analysis and cleansing were done using these generated documents. Figure 5.6 shows the result of this analysis.

As it can be seen, the number of words is higher for drivers than for impediments. This is related to the number of codes each category has as shown in Table 5.4. Moreover, it has to be remembered that for some companies certain aspects are seen either as drivers or impediments. A clear example of this is ”awareness”. Some companies with cyber insurance indicated that the lack of awareness about cyber risks was a reason to start considering cyber insurance. Whereas companies without cyber insurance indicated that they have a high degree of awareness about these topics.

[2]The grounded number indicates the number of times the code was applied.

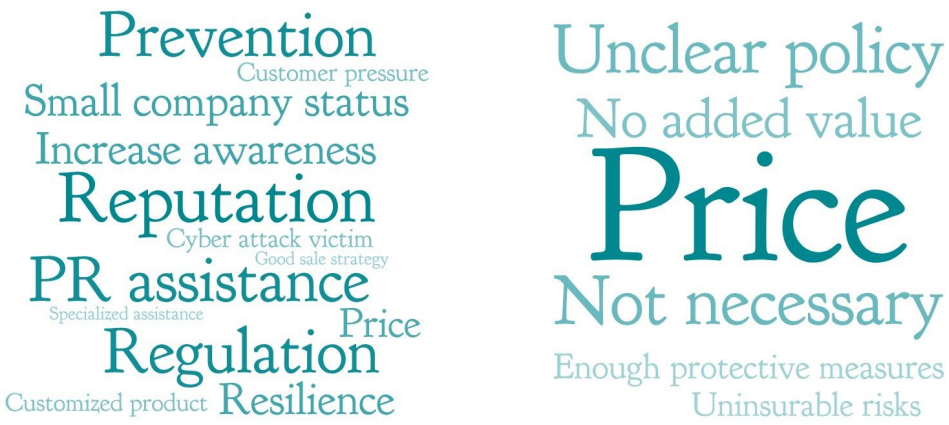


Figure 5.6: Drivers (left) and impediments (right) for cyber insurance adoption.

5.5. Summary of results

This section provides a summary of the results presented in this Chapter 5. Regarding PMT, the results are presented for the sources of information component and the two processes that form this theory, the threat appraisal and coping appraisal. For sources of information, the results are:

- ***Intrapersonal sources of information***. Most of the companies did not have previous knowledge about cyber insurance. The broker plays an active role creating awareness about the product. Only 2 out of 11 companies know other companies with cyber insurance.
- ***Environmental sources of information***. Only one of the companies has discussed cyber insurance with other companies. 5 out of 11 companies know companies that have suffered a cyber attack.

For the treat appraisal process, the results are:

- ***Vulnerability***. Digitalization, having the client's confidential information and reputation are the main factors that SMEs perceive make them susceptible to cyber attacks. The main protective measures in place are firewalls, identity and access management and business contingency plan.
- ***Severity***. Data leakage, service disruption, phishing, and ransomware are the security threats mentioned as the most critical threats.
- ***Rewards***. The main reasons for SMEs to not get cyber insurance are a high premium price, the perception that is not necessary to have it, and that they find the policy to be unclear regarding coverage and applicable claims.

For the coping appraisal process, the results are:

- ***Response efficacy***. For companies in Scenario I, insurers are not requesting additional security controls for companies to insure them. Regarding the expectations with cyber insurance, companies expect to get appropriate help in case of an attack but also expect not having to use the insurance. For companies in Scenario III, most of them consider they are implementing enough security controls to prevent or act against cyber attacks.
- ***Self-efficacy***. 3 out of 11 companies have suffered cyber attacks, causing business interruption and financial losses. For companies in Scenario I, they indicated that cyber insurance policy is understandable and clear. For companies in Scenario III, they consider having a good IT security management strategy. Most of them do not consider any noteworthy reason to get cyber insurance.
- ***Response cost***. Cyber insurance premium price is considered to be fair.

The business process identified in Section 5.2 reaffirmed the business process shown in Figure 3.4, in Chapter 3. The broker has an active role creating awareness among SMEs. The process does not take too long due to the low number of persons involved. Moreover, an internal process was identified, which can be influenced by the level of knowledge about information security of the personnel.

Section 5.3 found three additional topics usually mentioned during the interviews, cyber insurance market, cyber insurance validity (or novelty) and the moral hazard issue for companies with cyber insurance.

Finally, Section 5.6 shows how the generated codes are used to detect the most common driver and impediments for cyber insurance. The most common drivers are reputation, prevention, small company status and increase awareness. The most common impediments are price, unclear policy, and enough protective measures.

A total of 11 interviews were made to SMEs involved in the process of cyber insurance adoption. Three scenarios and three questionnaires were envisioned in this process, but the low number of interviews for Scenario II moved this research to only being able to show results for Scenarios I and III. Besides, the company in Scenario II had recently decided to get cyber insurance. The purpose of interviewing SMEs' representatives is to know the reasons that guided them to take or decline cyber insurance. According to theory, a way to research for these reasons is through behavioral theories like PMT, but the traditional business process should also be considered when analyzing a company's decision-making process. This chapter was mainly focused on showing the results regarding PMT, and the business process. These results will assist in answering the rest of the sub-research questions, and the research question to finally develop the decision-making model for cyber insurance adoption.

6

Discussion, conclusion and recommendations

The results presented in Chapter 5 are interpreted and described to approach towards answering the rest of the sub-research questions and the research question. First, a recapitulation and discussion of what has been learned about PMT and the construction of a decision-making model for cyber insurance adoption through this theory and the business process is in Section 6.1. To do this, the type of influence PMT and the business process have towards cyber insurance adoption are provided. These influences guide companies on deciding to get or not cyber insurance. After this, section 6.2 provides the answers to sub-research questions 3, 4 and 5, to finally guide the path to answer the research question in Sub-section 6.2.2, where the decision-making model for cyber insurance adoption, product of this research, is presented and explained. Sub-section 6.2.3 presents the final conclusions of the research. Then, Section 6.3 provides recommendations for researchers and the industry.

6.1. Discussion

Before answering the rest of the sub-research questions, the results showed in Chapter 5 are discussed to clear the path toward the final answers.

Threat appraisal

Companies acknowledge that digitalization is the main source of the threat since their information is exposed on the Internet, but they also recognize digitalization as necessary for their company to grow, then this is a risk they accept to take. This is also applicable to other vulnerability factors like client' confidential information and reputation because these are aspects necessary to carry out their business. With acceptable risks, protective measures must be considered. Most companies have IT and security services outsourced since they usually do not have specialized personnel to perform these activities, so they decide to leave it in the hands of professionals. Nevertheless, outsourcing IT and security services is also seen as a threat since the company is not in control of their resources. Finally, the main reasons for not getting cyber insurance are price and the perception that is not a necessary product. The latter reason is perceived because a cyber-attack has a low probability to happen, they have only seen attacks in the media but not in their network, their systems have been working without interruption for decades or because they do not see that an attack would have irreversible consequences.

Table 6.1 summarizes the reasons a company analyze when deciding on cyber insurance. In the figure, the positive or negative influence towards cyber insurance is related with the inclination of the company to take or not cyber insurance.

Without exception, the representatives mentioned different reasons for which their companies could be affected by a cyber attack. This is the beginning of the threat appraisal process. A crucial point where the companies' opinion regarding cyber insurance could flip comes when they analyze the state of their IT and security services. Companies that consider having experienced personnel and protective

		Positive	Negative
Digitalization PII Reputation	Acceptable risks	✓	✓
	Expert protective measures		✓
	Basic protective measures	✓	
	High premium price		✓
	Probability of the attack to occur	✓	✓

Table 6.1: Influence towards cyber insurance in the threat appraisal process

measures will hesitate more on getting cyber insurance. Whereas companies with basic protective measures do consider it practical to transfer their risks.

Coping appraisal

After the threat is identified, the company will analyze the possible ways to overcome it and how capable it is to put an adaptive response in place. For companies in Scenario I, cyber insurance is the analyzed adaptive response, whereas, for companies in Scenario III, their protective measures in place are the analyzed response.

Brokers have been executing an appropriate approach by first creating awareness about cyber risks and the ways to deal with them. Only after awareness has been raised do they start offering cyber insurance. Additionally, their collaboration with IT security companies and including them as part of the product gives added value to companies without specialized protective measures. The companies with cyber insurance indicated that the policy, its coverage, and damages covered are clear but more than that, the availability of external staff to assist them in case of an attack is considered an advantage for having cyber insurance. Price could be an essential reason, but none of the companies with cyber insurance expressed complaints about it, and it is recognized that the price could go lower.

In this stage, protective measures are once again analyzed by the companies to make a comparison between what they have and what is offered. For companies in Scenario III, they consider to have proper security management in place and be able to prevent or act on time if a cyber attack occurs. Also for these companies, if cyber insurance is to be considered, the price is an important element to analyze, but more important is that they perceive specific risks to be uninsurable and not possible to cover with insurance, like reputation, or going out of business because of a breach. Table 6.2 summarizes the elements a company analyzes if they are capable of coping with cyber threats through their own protective measures or by means of cyber insurance.

Towards a decision-making model

A decision-making model can start to be developed with the type of influence created by the threat appraisal and coping appraisal components. A positive influence will push an SME to acquire cyber insurance, whereas the negative influence will do the opposite. The first component to consider is **sources of information**. From the results, the intrapersonal and environmental sources of information can have an active or passive role. The active role appears when companies without experience in dealing with cyber attacks protection directly know other companies that have suffered a cyber attack. Another active role comes when the broker is creating awareness among companies regarding cyber risks. The passive role is informative, especially the media coverage of cyber attacks.

As it has been indicated, the PMT **threat appraisal** starts when fear is perceived, this is going to be named the "company's perceived exposure to risks". After this, the threat appraisal process is initiated with the company evaluating the protective measures it has in place. With this information, the company can measure the probability of an attack to occur, the perception can be that the risks are acceptable or uninsurable.

		Positive	Negative
	Clear policy and prompt assistance	✓	
	Able to deal with cyber attacks		✓
	Fair price	✓	
Reputation Going out of business	Uninsurable risks		✓

Table 6.2: Influence towards cyber insurance in the coping appraisal process

When the threat appraisal process finishes come the **coping appraisal** process with the analysis of the offered policy coverage. If the policy is clear for the SME and provides additional services like prompt and professional assistance, the company will perceive the added value of the insurance. In the coping appraisal process, financial costs (the premium price) are considered. As shown during the interviews results, a high premium price would be an automatic cause for not selecting cyber insurance.

If after threat appraisal and coping appraisal processes the company is still interested in cyber insurance, the **business process** will appear. The internal process identified in Section 5.2 is also present. The outcome from these processes can be either to get or decline cyber insurance. These outcomes depend on the SME' decision-makers' priorities for the company and company guidelines. A summary of the analyzed elements and the influence towards cyber insurance adoption is in Table 6.3.

Process	Element in decision-making model	Positive	Negative
Sources of information	Communication networks	✓	
Threat appraisal	Protective measures	✓	✓
	Probability of occurrence of the attack	✓	✓
	Acceptable risks	✓	
Coping appraisal	Policy coverage	✓	
	Added value	✓	
	Premium price	✓	✓
	Uninsurable risks		✓
Business process	Evaluation of alternatives to insurance	✓	✓
	Evaluation of insurance services	✓	✓

Table 6.3: Influence towards cyber insurance adoption

6.2. Conclusion

6.2.1. Answers to sub-research questions 3, 4 and 5

The rest of the sub-research questions can be answered after semi-grounded techniques, and qualitative analysis of the results has been done.

SQ3: How does threat appraisal influences cyber insurance adoption and the decision-making process? PMT indicates that for an individual to get protection against a threat, the threat first needs to be detected. Through the vulnerability element, companies recognize they are susceptible of being attacked, but the severity of the impact differs depending on their main business activities. Companies will accept the risks that come with digitalization and will try to implement protective measures. The rewards element identified the reasons companies have for not acquiring cyber insurance, where price and the perception that it is not necessary were the most common answers. A summary of the influence the threat appraisal has is in Table 6.1.

During the decision-making process, the maturity of the protective measures could flip the company's decision. Expert protective measures lean the decision to consider cyber insurance not to be necessary, but basic protective measures will help to consider it as an appropriate way to transfer risk. Overall, the main asset they want to protect is their reputation.

SQ4: How does coping appraisal influences cyber insurance adoption and the decision-making process?

After the threat is identified, the company will analyze the possible ways to overcome it (response efficacy element) and how capable it is to put an adaptive response in place (self-efficacy element). If the company is considering cyber insurance, it will be important for them to have an insurance policy that is clear regarding the coverage and the cases when claims can be made. Moreover, services like 24/7 assistance and legal advice will provide additional reasons for the company to feel inclined towards cyber insurance. If a company perceives to be able to deal with cyber attacks and sees no added value in the cyber insurance offer, it will feel inclined to continue protecting itself with the measures it has in place. Regarding the response cost element, for all the companies the premium price plays a role, but the majority of SMEs with cyber insurance expressed that the price is fair. A summary of the influence the coping appraisal has is in Table 6.2.

During the decision-making process, the companies analyze the cyber insurance policy details and determine if it provides additional value for their companies. Additionally, the premium price could flip the company's decision in favor (if it is considered to be fair) or against (if it is considered to be high) of cyber insurance adoption.

SQ5: What are the drivers and impediments for SMEs to get cyber insurance?

In Section 5.4, the most mentioned drivers and impediments from the interviews are indicated. Regarding the drivers, reputation is the main asset companies will try to protect through different options, one of them being risk transfer. Companies indicated they do not perceive to be the primary target of hackers. Nevertheless, prevention is crucial due to the increase of commoditized attacks. SMEs character implies they do not have a big budget or specialized personnel to handle different IT security measures if this is not their core business. Finally, companies recognized that cyber insurance had increased their level of awareness and because of this, they cannot be blind to potential risks.

Two drivers playing an essential role in cyber insurance adoption are regulation and customer pressure. The term regulation is used to refer to sectorial recommendations made to a couple of companies and the influence GDPR had in one company. Customer pressure was indicated by one of the companies in Scenario III as a potential scenario where they would consider getting cyber insurance. After this, drivers can be listed as the most mentioned and the definitive drivers, the latter refers to those drivers that without considering the most mentioned reasons, will prevail in the company's decision. The list is shown in Figure 6.1.

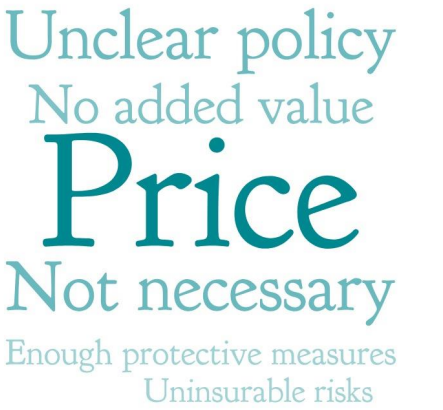
For impediments, price is the main reason to decide not to get cyber insurance. Besides this, an unclear policy and having enough protective measures are the most mentioned reasons. For the first, if the process with the broker is long and complicated, SMEs will not want to continue with it. Also, if the coverage is not detailed enough, it will make the companies feel that the insurance is not going to work as promised. Regarding enough protective measures, this reason was mainly mentioned by IT companies. Since their understanding of the cyber security ecosystem is vast and their business

Most mentioned	Definitive reason
Reputation	Regulation
Prevention	Customer pressure
Small company status	
Increase awareness	

Figure 6.1: Drivers for cyber insurance adoption

activities make them have specialized personnel, they would feel able in preventing and acting on time against cyber attacks.

There is one isolated case where a definitive reason was found. A company indicated two reasons for not getting cyber insurance. The first is, they consider reputation to be an uninsurable risk, the other one is that this is an outsourcing company on behalf of a larger one. This situation makes them not to be responsible for any financial loss because the large company has the responsibility to protect the small one. The fact that a large company takes care of them makes it the primary reason for not getting cyber insurance, as stated by the interviewee. This situation was not mentioned in Chapter 5: Results since the company's status does not correspond to the questions related with PMT or the business process. The given name to this situation is "protective parent company". Finally, a similar relation can be made as with the drivers, where a differentiation between the most mentioned and the definitive reasons for not getting cyber insurance are listed in Figure 6.2.



Most mentioned	Definitive reason
Price	Protective parent company
Unclear policy	
Enough protective measures	

Figure 6.2: Impediments for cyber insurance adoption

6.2.2. Answer to research question

What decision-making process do SMEs follow to acquire cyber insurance?

In the end, everything comes down to understanding the process and the elements involved for SMEs to decide whether or not cyber insurance is worth having. The beginning of this chapter explained the influence PMT components and the business process have towards cyber insurance adoption, with a summary in Table 6.3. This table guides the decision-making model shown in Figure 6.3. This model is the final result of this research. Theory showed at the beginning that the decision to get cyber insurance could not be only guided by rational thinking like a business process. Then, PMT appeared to be able

to explain the missing irrational aspect not identified in the business process. However, only applying PMT in the decision-making process of a company leaves out the policies and procedures existing in any company. The outcome of the theory research is to identify the three processes present during a decision-making process for insurance, which are the emotional, cognitive and business processes. The structure of the model is explained below.

For sources of information component, it can have an active or a passive role. An active role would come if the company directly knows other companies that have suffered a cyber attack. Otherwise, the role of this element would be informative, especially the media coverage about cyber attacks.

For the threat appraisal component, there is an element that can be decisive, the state of the security protective measures. Expert protective measures lean the decision to not getting cyber insurance, but basic protective measures will make the company consider cyber insurance. Then, the company will analyze the probability of the attack to occur. The outcome can be to accept the risk and continue with the analysis, or consider that the risk are uninsurable, which will cause the company to not get cyber insurance.

For the coping appraisal component, the company analyzes the policy coverage, focusing on the added value it offers. In this process there is also an element that can be decisive, the premium price. If it is too costly, the company will decide not to take the cyber insurance.

Regarding business process, the first stage, ”Evaluation of alternatives to insurance” will involve either one or more persons, and it will be the stage where the offer is brought to the decision-maker of the company. After this, additional evaluation of the product could be done internally before deciding to get the product or not at the ”Evaluation of insurance services” stage.

6.2.3. Final conclusion

This research started by looking at the big picture about the increase of cyber attacks, its effects, and how companies are dealing with them. Then it focused in a section not carefully examined since it has not been the main target of cyber security attacks, the SMEs. Commoditized attacks are growing and even though these type of attacks do not have significant financial impacts as high-end attacks, they can be easily spread and affect more persons or companies.

Cyber insurance is one of the ways to deal with cyber risks by transferring the risk to a third party, but its development has been slow, especially when is compared to the U.S. This research took the opportunity to go out and make on-field research to discover the reasons for this behavior and the different stages an SME follows to make the final decision.

PMT proved to work adequately as a backbone theory to understand the processes and elements involved when a decision-maker needs to take action about protecting its company against cyber risks. Even that PMT was used in the context of SMEs decision-making due to their size and the limited number of people involved in the process, it should not be forgotten that SMEs still need to comply with policies and procedures present in a company. This is the reason for which the decision-making model provided product of this research is considering PMT components and the business process. Moreover, the model provides flexibility in its use as it usually occurs when individuals make decisions. Some decision-makers will follow all the process and analyze every element to make a decision, and others will stop in specific steps guided by their own beliefs and the company’s priorities. To the best of knowledge of the researcher, this is the first decision-making model for cyber insurance adoption focused on SMEs that has been done.

6.3. Recommendations

Along with this research, theory and empirical research provide the opportunity to make general recommendations to researchers wanting to do similar research and to the industry.

6.3.1. Recommendations for researchers

Since the main source of information came from the semi-structured interviews, recommendations can be provided for researchers wanting to embark on this complicated but fruitful task.

- Do not stop insisting in your objective to get the interview until you get an answer (either positive or negative). Mails, phone calls, voicemails, reminders, and LinkedIn are valid means.

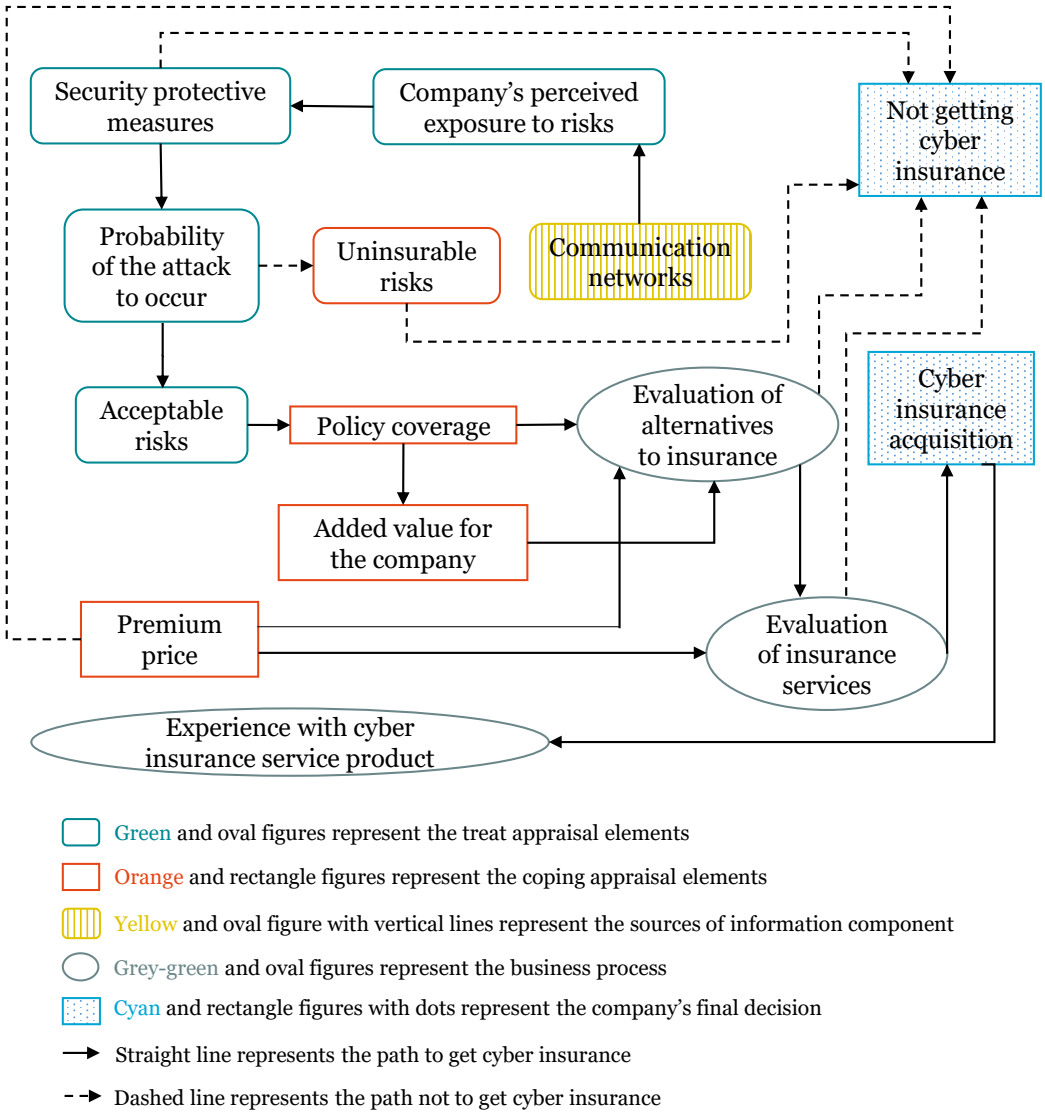


Figure 6.3: Decision-making model for cyber insurance adoption

- Take into consideration time and cost factors in your research. If there are limitations regarding these points but the researcher still prefers to have face-to-face interviews, consider letting know your contacts (in this case, the broker) the reachable geographical areas.
- Start transcripts as soon as possible to remind any misunderstanding that could be detected from the audio recording.
- Indicating the academic nature of the work is important when dealing with the industry. The mindset and objective of each side is different. Then, is important for both sides to be clear on the purpose of the interview and how the data will be used.

6.3.2. Recommendations for the industry

Interviews with SMEs's representatives gave insights to make practical recommendations to both the supply and demand sides of the cyber insurance market. The reader should bear in mind that these recommendations are the result of the knowledge gathered from the interviews and literature review, and not from a complete study of the cyber insurance market.

Recommendations for the supply side of the cyber insurance market

- Show clients the continuous decline of cyber insurance premium prices. If future premium prices are expected to continue this trend, it would be more favorable to be shown. As it was extracted from the interviews, current cyber insurance holders took great consideration of this fact.
- Expectations from the companies regarding cyber insurance are high, as it was shown in the results for the response efficacy element. Nevertheless, checking security controls did not appear as a common practice from the broker. Applying security controls (an example can be found in (Woods et al., 2017)) could be useful to comply with the client's expectations.
- Provide specialized training to sales representatives for cyber insurance, soft skills to deal with technical terminology is relevant.
- Continue creating events/forums where companies that have suffered a cyber attack can expose their case and allow guests to approach to them to discuss it.
- Assist companies to bring the message to decision-makers. Provide them information like charts with price evolution and trends in the cyber security field in a way that managers can easily understand.
- To avoid moral hazard, assist the company in creating an educational program to raise awareness among the employees.

Recommendations for the demand side of the cyber insurance market

- Avoid making decisions under stressful circumstances (for instance, immediately after suffering an attack) since an emotional reaction would mainly guide it.
- If IT services are outsourced, procure having it with companies with expertise in cyber security, and regular checks like penetration tests are included.
- When exists previous collaboration with the broker, and there is a high degree of trust, the amount of effort to research about new products, like cyber insurance, is reduced.
- Require security control checks from the insurer, this would add a preventive measure for the sake of the company.

The end of the thesis is near. This Chapter presents the most important outcome, the decision-making model for cyber insurance adoption, which is the result of the methods and effort applied in this research. At the beginning of the Chapter, a discussion about the results gathered in Chapter 5 clears the path to answering the rest of the sub-research questions. The discussion section provided a series of elements to take into account when the decision-making process for cyber insurance adoption is executed. The tags gave for positive and/or negative influence should only be understood in the context of the mentioned process. Finally, it is considered that the knowledge gathered through this research can lead to practical recommendations to be taken into account by researchers and the industry.

7

Reflection

In this chapter, the research outcome and process are holistically reviewed. It has been decided to call it Reflection, though it also contains the limitations of the research in Section 7.1, and recommendation for future research in Section 7.2. This decision was made because the objective of the chapter is to take a step back and provide a discussion about what has been learned. Additionally, each section is linked with each other, where the outcome is a reflection of the project.

7.1. Limitations of the research

Every research method has its advantages and limitations. The chosen methods lead to results with their limitations. In the following paragraphs, the limitations are discussed per method.

Literature review. A vast number of academic research about cyber insurance adoption is lacking. The existing literature comes with flaws since the reliability of sources can be questioned due to the impossibility to compare results from diverse sources across them. When searching for literature related to SMEs, the number of available researches drop even more. Nevertheless, big consultancy firms are taking a step forward to fulfill this gap. Research from Capgemini (2017), and Deloitte (2017) from last year is starting to consider the SMEs sector. Regarding the literature review about PMT, the limitations are in the qualitative research, whereas the quantitative studies using PMT are numerous. Nevertheless, works like (Posey et al., 2014) helped to realize how qualitative research using PMT is done.

Semi-grounded theory. The exposed limitations on literature review paved the way towards choosing semi-grounded theory for data analysis. Conveniently, not going too deep in the literature review is one of the requirements of this theory. An important limitation came when deciding how to implement the semi-grounded theory techniques. Traditional research implements qualitative software like Atlas.ti, NVivo and MAXQDA. Then, this seemed to be the natural approach for this research as well. Although the software assists by having a structured workplace and quick access to the interviewees' quotations after they have been coded, it has its disadvantages when working with a sample size of 11 interviews. As it was shown in Chapter 5, on some occasions the software helped to find results related to the PMT elements quickly. For instance, for the severity element, phishing and data leaks were the most cited answers, but when the vulnerability element was reported, the researcher could not rely on the absolute values of the times a word or a sentence was mentioned in the interviews. For this and more cases, a manual analysis had to be performed, which can be done with a small sample size. However, when bigger samples size is present, manual analysis is not recommended. It also has to be mentioned that at the beginning of the research, it was envisioned a larger number of interviews, this was another reason for choosing the software as a means for data analysis.

Semi-structured interviews. It is considered that the background every respondent has was helpful for the objective of the research since all of them were involved in the decision-making process regarding cyber insurance. The main limitation came with the discussion about protective measures. For respondents who do not have a background in information security it is hard or even impossible to discuss this topic in detail. Moreover, the inability to reach sufficient interviewees for Scenario II was relevant for not providing an analysis where the three scenarios could be compared.

7.2. Future research

In the following section, recommendations for further research on the topic of cyber insurance adoption among SMEs is presented.

- The decision-making model is the main outcome of this research and it follows the process explained by the interviewed companies. Nevertheless, this model will have to be validated with more SMEs. First, it is considered that a focus on Dutch SMEs is more appropriate, and it is suggested to expand the focus to include other countries within the EU.
- The questionnaire used in this research could be used to gather additional data, which means, performing more interviews. New data will help identifying differences between the scenarios defined in this research and to identify differences between sectors. IT was the sector with the largest number of participants, but the results showed that their views are different from the rest of the sectors. Since IT is not the most representative sector for Dutch SMEs, their views need to be considered.
- A quantitative approach has commonly been applied to PMT research. Then, additional research using this focus could be followed, but researchers should be careful about selecting the audience. This type of research needs a large sample size which can lead to a reduction of the meaningful information participants could provide.
- From the point of view of policymakers, research could be performed about the impact regulatory frameworks can make for cyber insurance adoption. As it was shown in the Results, a couple of companies took with deep care the recommendations made by their sectorial group. This could be further translated into regulation.
- A questionnaire like the one used in this research can always be improved. In the next section about Reflection, the questionnaire is discussed, where suggestions are made regarding certain questions. These suggestions could be followed for further research, and additional suggestions should be introduced to avoid misinterpretations about the questions. Consequently, the questionnaire can be further improved to become a more reliable tool.
- PMT was chosen among different behavioral theories; a comparison with the rest of the behavioral theories could be done to test if PMT is the best approach to analyze the decision-making process for cyber insurance adoption.
- Since SMEs only count for 2% of the cyber insurance market, the research could be extended to companies that do not employ cyber insurance as part of their portfolio. In order to continue investigating the different approaches to decision-making, the research should be focused on investigating the PMT elements and business process with similar insurance like liability insurance.

7.3. Reflection

The section has been divided into three parts, the reflection about the choices made within the project, the academic and societal reflection related to what was presented in Section 1.5, and the personal reflection with the vision of a CoSEM student.

7.3.1. The choices made

The questionnaire

The results gathered reinforce the use of PMT as a theory to research the process companies follow to evaluate threats and selecting the alternatives to handle this threat. Every PMT element was useful for the development of the questionnaire mainly by helping to understand the theory and the context of cyber security and cyber insurance. The next paragraphs indicate the main aspects detected of the questionnaire that should be improved.

The question ”Do you think some of the threats have more impact than others?” did not give additional information. The question that goes before this one, ”What are the main security threats you consider relevant to the company?”, provided the answer regarding the degree of severity.

For companies in Scenario I there is a question about the protective measures they have besides cyber insurance (for the vulnerability element), and another question to know if the broker asked for additional security controls (for the response efficacy element). Nevertheless, a question is missing to know if the company considers it needs additional security controls (also for the response efficacy element). This last question was included in the questionnaire for the companies in Scenario III. The decision for not including the question about additional security controls was made to avoid redundancy in the type of questions made. Nevertheless, it is considered that a question like this would be worth including to provide the companies the opportunity to discuss a future scenario about the investments they should do to protect themselves against cyber attacks.

Although the questionnaire had already been arranged and the script planned, during the interview, there was room to improvise. It usually happened that the interviewee started mentioning topics before they were planned in the discussion. For these cases, the researcher should be careful to follow the thread and keep the momentum to allow the interviewee to express his views.

The qualitative software

The amount of interviews provides the option to do a qualitative analysis without the assistance of software. Using the software felt unnecessary at times because the coding, coding structure and forming the groups followed a repetitive process to make sure not leaving important sentences behind. Moreover, the software was used in parallel with manual analysis, putting information in an Excel file to then contrast it with the results provided by the software. Nevertheless, having a quantitative proof when a topic is constantly repeated gives additional tools to support the findings, instead of only relying upon the qualitative result.

The project process

Doing research like this requires countless time and effort. The central aspect hampering its realization besides the inherent difficulties of doing a Master thesis was the set-up of the interviews. It was not envisioned in the beginning that getting SMEs to participate would be so complicated in terms of time and willingness. It was relatively straightforward getting interviews with the supply side, meaning mainly brokers, but their willingness to participate was much higher than the one of SMEs. In this sense, future researchers wanting to follow a similar approach should plan with months in advance the list of potential contacts to interview. Additionally, from the period of time the research was done, it was learned that vacation periods should be avoided since response rate will most likely decrease.

7.3.2. Scientific and societal reflection

The scientific relevance of this thesis is firstly ensured by the decision-making model. The model is unique in the way that it probes real behavior by SMEs when they are considering adopting cyber insurance since it was obtained from practical experience from the companies. It allows a dynamic use by showing the main stages as companies do not have the will to focus in the whole process but prefer to give a more significant weight to specific elements. It can be the case that a company does not have enough budget, so they immediately decide not to consider adopting the insurance, or it could be the case where a company values its IT and security management strategy so high that no added value is seen in products like cyber insurance.

Second, using PMT as a backbone theory to develop the model gives the opportunity to include the irrational aspects present when decisions under risk are made. In the decision-making model PMT elements guide the first stages of the process, and then, the internal decision-making processes occur, which will vary depending on the company priorities and guidelines. This research has added theory contribution to the use of PMT in qualitative research since its implementation had only been made with quantitative methods before. An additional contribution is provided to the cyber insurance adoption field, where the research has been based so far on mathematical models.

Regarding the societal relevance, the drivers and impediments that were identified, provide a better understanding of the priorities SMEs have, which can lead to the offer of better services and products. Still, more data should be gathered through similar interviews like the it was done in this research to better understand the Dutch SME sector.

Moreover, the active role the broker is having creating awareness about cyber risks probed to have positive consequences. This could be seen through the adoption of cyber insurance and the effort companies are making to have strong protective measures in place to prevent any potential attack.

The more awareness is created among society, in this case through SMEs, has a positive impact in a world where the dependence on digital communications is undeniable. As it was stated in section 1.5, since SMEs are responsible for the employment of 65% of the people in the Netherlands, the impact they can create is enormous.

Finally, the decision-making model provides holistic, understandable elements into cyber insurance adoption for the SMEs wanting to implement it, and for the rest of the actors wanting to understand this process.

7.3.3. Personal reflection

This thesis marks the end of the MSc. program CoSEM. In short, the CoSEM program is centered in the analysis and design of complex socio-technical systems within a specific track, Information and Communication for my case. Selecting this track was done with the focus on widening my knowledge about cyber security. Doing this research proved to be a great challenge since behavioral psychology is not part of my professional background. Nevertheless, this is part of the purpose of being a CoSEM student, be able to apply technical knowledge into different areas. The thesis is strongly linked to the Master program by analyzing a complex socio-technical system, the cyber insurance ecosystem. The technical issues were analyzed in the beginning to understand the difficulties of the implementation of such a product. Besides, the institutional difficulties were addressed from the point of view of organization structure and actor's behavior for cyber insurance adoption. Furthermore, the decision-making model is the result of the design of a characteristic for such a complex system.

Studying research related to the application of PMT for insurance adoption guided the questionnaire design process. Before applying PMT, the background was based on literature review and previous knowledge. After including PMT, questions had a broader meaning and background, which was extremely useful when interviews were done. Furthermore, an exciting discovery was while doing the interviews. In the beginning, I did not anticipate the personal knowledge and experience I would get from the interviews. The information gathered from the personal and professional experience of the interviewees gave additional insights that I am sure would not be possible to get from methods like literature review, I hope the report is presenting this fruitful information that was provided.

When doing research for a MSc. thesis is easy to be deeply involved in the topic, focusing only on achieving the outcomes. Hopefully, this chapter was able to provide a different perspective on what is left to investigate by analyzing what has been learned during this process, (yes, process). The limitations in Section 7.1 were discussed in terms of the methods used in the research. Then, Section 7.2 gives recommendations for future research related to what has been presented in this thesis. Some of these recommendations are directly linked with the limitations, and the rest were identified during the realization of the project. Finally, the Reflection in Section 7.3 is provided for three aspects. First, regarding the choices that were made for this project, its execution and the use of the qualitative software. Second, the scientific and societal view presented in Chapter 1. Finally, a personal reflection as a CoSEM student is given.

References

AIG. (2017). *Demand for cyber cover among SMEs on the rise in Benelux as GDPR deadline looms.* Retrieved from https://www.aiginsurance.nl/insights/demand-for-cyber-cover-among-smes-on-the-rise-in-benelux-as-gdpr-deadline-looms

Ajzen, I. (1991). The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.*, *50*(2), 179–211. doi: 10.1016/0749-5978(91)90020-T

Akerlof, G. A. (1970). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *Q. J. Econ.*, *84*(3), 488. Retrieved from https://academic.oup.com/qje/article-lookup/doi/10.2307/1879431 doi: 10.2307/1879431

Autoriteit Persoonsgegevens. (n.d.). *Tasks and powers of the Dutch DPA.* Retrieved from https://autoriteitpersoonsgegevens.nl/en/node/1930

Axelrod, L. J., & Newton, J. W. (1991). Preventing Nuclear War: Beliefs and Attitudes as Predictors of Disarmist and Deterrentist Behavior. *J. Appl. Soc. Psychol.*, *21*(1), 29–40. doi: 10.1111/j.1559-1816.1991.tb00440.x

Bandyopadhyay, T., & Shidore, S. (2011). Towards a managerial decision framework for utilization of cyber insurance instruments in IT security. In *17th am. conf. inf. syst. 2011, amcis 2011* (Vol. 2, pp. 1397–1405). Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84870215709{&}partnerID=40{&}md5=a4581e0a79a073194716976cd8916e76

Bonner, M. (2018). *How Insurance Agents and Brokers Make Money.* Retrieved from https://www.thebalancesmb.com/agents-versus-brokers-and-how-they-make-money-462383

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015, dec). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Q.*.

BPF Cybersecurity. (2017). *IGF 2017 - Best Practice Forum on Cybersecurity.* Retrieved 2018-03-10, from https://www.intgovforum.org/multilingual/content/igf-2017-best-practice-forum-on-cybersecurity

Bradford, J. (2015). *Advisen Insight: Cyber insurance market update.* Retrieved from https://www.advisenltd.com/2015/01/15/advisen-insight-cyber-insurance-market-update/

Busenitz, L. W., & Barney, J. B. (1997). *Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making.* doi: 10.1016/S0883-9026(96)00003-1

Capgemini. (2017). *Trends in Cybersecurity 2017-2018* (Tech. Rep.). Netherlands: Capgemini Nederland B.V. Retrieved from https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2017/11/trends-in-cybersecurity{_}1b-105-17.pdf

Chinn, D., Kaplan, J., & Weinberg, A. (2014). Risk and responsibility in a hyperconnected world: Implications for enterprises. *World Econ. Forum Collab. with McKinsey Co.*(January), 1–40.

Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Crim. Justice Stud. A Crit. J. Crime, Law Soc.*, *28*(3), 336–355. Retrieved from http://dx.doi.org/10.1080/1478601X.2015.1050590 doi: 10.1080/1478601X.2015.1050590

Cox, D. (2017). *Managed IT Services - The Ultimate SME Guide to Selecting a Provider.* Retrieved from https://www.zsah.net/managed-it-services

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation). doi: oclc/56932490

De Bruijn, H., & Ten Heuvelhof, E. (2012). *Management in networks: On multi-actor decision making*. doi: 10.4324/9780203885666

De Smidt, G., & Botzen, W. (2018). Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *Geneva Pap. Risk Insur. Issues Pract.*, *43*(2), 239–274. doi: 10.1057/s41288-018-0082-7

Deloitte. (2017). *Dealing efficiently with cybercrime. Cyber Value at Risk in The Netherlands 2017* (Tech. Rep.). Deloitte The Netherlands.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law Soc. Chang.*, *67*(1), 97–116. Retrieved from http://dx.doi.org/10.1007/s10611-016-9649-z doi: 10.1007/s10611-016-9649-z

Enserink, B., Hermans, L., Kwakkel, J., Thissen, W., Koppenjan, J., & Bots, P. (2010). Policy Analysis of Multi-Actor Systems. *Lemma*.

European Commission. (n.d.). *What is an SME? - European Commission.* Retrieved from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition{_}en

European Union. (n.d.). *About the EU.* Retrieved from https://europa.eu/european-union/about-eu{_}en

European Union. (2003). EU Recommendation 2003/361/EC. *Off. J. Eur. Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361{&}from=EN

Financier Worldwide. (2015). *A new approach to risk assessment for cyber insurance.* Retrieved from https://www.financierworldwide.com/a-new-approach-to-risk-assessment-for-cyber-insurance/{#}.W21scNIzaMp

Fisher, S. (2014). *How to Calculate the Cost of a Target Breach At Your Company.* Retrieved 2018-02-27, from https://www.laserfiche.com/simplicity/how-calculate-cost-target-breach-your-company/

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *J. Appl. Soc. Psychol.*, *30*(2), 407–429. doi: 10.1111/j.1559-1816.2000.tb02323.x

Fox. (2016). *JPMorgan data breach adds to concern over security of consumer data at banks, retailersle.* Retrieved 2018-02-27, from https://www.foxbusiness.com/features/jpmorgan-data-breach-adds-to-concern-over-security-of-consumer-data-at-banks-retailers

Franke, U. (2017). The cyber insurance market in Sweden. *Comput. Secur.*, *68*, 130–144. doi: 10.1016/j.cose.2017.04.010

Glenk, K., & Fischer, A. (2010). Insurance, prevention or just wait and see? Public preferences for water management strategies in the context of climate change. *Ecol. Econ.*. doi: 10.1016/j.ecolecon.2010.06.022

Government of the Netherlands. (n.d.). *Information from the Government of The Netherlands.* Retrieved from https://www.government.nl/

Grothmann, T., & Reusswig, F. (2006). People at risk of flooding: Why some residents take precautionary action while others do not. *Nat. Hazards*. doi: 10.1007/s11069-005-8604-6

Gurung, A., Luo, X., & Liao, Q. (2009). *Consumer motivations in taking action against spyware: An empirical investigation* (Vol. 17) (No. 3). doi: 10.1108/09685220910978112

Hackett, R. (2017). *Equifax Breach Affects 2.5 Million More People Than First Reported.* Retrieved from http://fortune.com/2017/10/02/equifax-credit-breach-total/

Hager, B. (2016). *The Role of the Managing General Agent.* Retrieved from https://expertinsurancewitness.com/the-role-of-the-managing-general-agent/

Hayel, Y., & Zhu, Q. (2015). Attack-aware cyber insurance for risk sharing in computer networks. In *Lect. notes comput. sci. (including subser. lect. notes artif. intell. lect. notes bioinformatics)* (Vol. 9406, pp. 22–34). doi: 10.1007/978-3-319-25594-1_2

Hemenway, C. (2015). *Cyber insurance market to reach $10B by 2020.* Retrieved from https://www.advisenltd.com/2015/07/30/abi-research-cyber-insurance-market-to-reach-10b-by-2020/

Hovav, A., & D 'arcy, J. (n.d.). The Impact of Virus Attack Announcements on the Market Value of Firms. Retrieved from https://www.tandfonline.com/doi/pdf/10.1201/1086/44530.13.3.20040701/83067.5?needAccess=true

Huth, M. (2018). *GDPR Compliance: Essential Training.* Linkedin Learning. Retrieved from https://www.linkedin.com/learning/gdpr-compliance-essential-training/next-steps

Ian Faulconbridge, R., & Ryan, M. J. (n.d.). *Systems engineering practice*.

Insurance Europe. (n.d.). *Insurer's role in increasing cyber resilience.* Retrieved from https://www.insuranceeurope.eu/cyber-insurance

Jones, J. a. (2005). An Introduction to Factor Analysis of Information Risk. *Risk Manag. Insight*, *1*(614), –. doi: 10.1037/h0038787

Kahneman, D. (2011). *Thinking , Fast and Slow*.

Kunreuther, H., & Pauly, M. V. (2018). *Dynamic Insurance Decision-Making for Rare Events: The Role of Emotions* (Vol. 43) (No. 2). doi: 10.1057/s41288-017-0068-x

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *Eur. J. Inf. Syst.*, *18*(2), 177–187. doi: 10.1057/ejis.2009.11

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Inf. Manag.*. doi: 10.1016/S0378-7206(01)00143-4

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. *Adv. Exp. Soc. Psychol.*, *5*(C), 119–186. doi: 10.1016/S0065-2601(08)60091-X

Loohuis, K. (2018). *Dutch SMEs' cyber security is insufficient.* Retrieved from https://www.computerweekly.com/news/252437551/Dutch-SMEs-cyber-security-is-insufficient

Meland, P. H., Tøndel, I. A., Moe, M., & Seehusen, F. (2017). Facing uncertainty in cyber insurance policies. In *Lect. notes comput. sci. (including subser. lect. notes artif. intell. lect. notes bioinformatics)* (Vol. 10547 LNCS, pp. 89–100). doi: 10.1007/978-3-319-68063-7_6

Morgan, S. (2015). *Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020.* Retrieved 2018-03-06, from https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity - market-reaches-75-billion-in-2015 - expected-to-reach-170-billion-by-2020/{#}294e9a1c30d6

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decis. Support Syst.*. doi: 10.1016/j.dss.2013.04.004

OECD. (2017). *Enhancing the Role of Insurance in Cyber Risk Management* (Tech. Rep.). Author. Retrieved from http://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management{_}9789264282148-en

Opdenakker, R. (2006). Advantages and disadvantages of four interview techniques in qualitative research. *Forum Qual. Sozialforsch.*. doi: 10.1177/1468794107085298

O'Reilly, M., & Parker, N. (2012). 'Unsatisfactory Saturation':A critical exploration of the notion of saturated sample sizes in qualitative research. *Qual. Res.*. doi: 10.1177/1468794112446106

Pandya, V. M. (2012). Comparative analysis of development of SMEs in developed and developing countries. *Int. Conf. Bus. Manag.*.

Ponemon Institute. (2017). *2017 Cost of cyber crime study. Insights on the security investments that make a difference* (Tech. Rep.). Ponemon Institute LLC. Retrieved from https://www.accenture.com/t20170926T072837Z{_}{_}w{_}{_}/us-en/{_}acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Inf. Manag.*. doi: 10.1016/j.im.2014.03.009

PUM Netherlands. (n.d.). *Business Support Organisations (Chambers/Associations).* Retrieved from https://www.pum.nl/business-support-organisations-chambersassociations

PwC. (2015). *Insurance 2020 & beyond: Reaping the dividends of cyber resilience* (Tech. Rep.). Author.

Reynaud, A., Aubert, C., & Nguyen, M. H. (2013). Living with floods: Protective behaviours and risk perception of vietnamese households. *Geneva Pap. Risk Insur. Issues Pract.*. doi: 10.1057/gpp.2013.16

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *Work. Econ. Inf. Secur.*, 1–40. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract{_}id=2929137

Sanner, M. (1994, apr). Attitudes toward organ donation and transplantation. a model for understanding reactions to medical procedures after death. *Soc. Sci. Med.*.

Schafer, R. B., Schafer, E., Bultena, G. L., & Hoiberg, E. O. (1993). Food safety: An application of the health belief model. *J. Nutr. Educ.*, *25*(1), 17–24. doi: 10.1016/S0022-3182(12)80183-X

Seidman, I. (2006). *Interviewing as Qualitative Research A Guide for Researchers in Education and the Social Sciences.* doi: 10.1037/032390

Song, X., Peña-Mora, F., & Arboleda, C. (2010). The application of utility theory in the decision-making process for investing in ADR insurance. In *Constr. res. congr. 2010 innov. reshaping constr. pract. - proc. 2010 constr. res. congr.* doi: 10.1061/41109(373)129

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decis. Support Syst.*, *75*, 49–62. doi: 10.1016/j.dss.2015.04.011

Stol, K.-j., Ralph, P., & Fitzgerald, B. (2016). Grounded Theory in Software Engineering Research : A Critical Review and Guidelines. *Proc. 38th Int. Conf. Softw. Eng. - ICSE '16*(Aug), 120–131. doi: http://dx.doi.org/10.1145/2884781.2884833

Sun, Y., Wang, N., Guo, X., & Peng, Z. (2013). Understanding the acceptance of mobile health services: A comparison and integration of alternative model. *J. Electron. Commer. Res.*.

TEDx. (2013). *Risk literacy: Gerd Gigerenzer at TEDxZurich.*

The European Commission. (2017). 2017 SBA Fact Sheet Netherlands. *Annu. Rep. Eur. SMEs*.

Tøndel, I. A., Seehusen, F., Gjære, E. A., & Moe, M. E. G. (2016). Differentiating cyber risk of insurance customers: The insurance company perspective. In *Lect. notes comput. sci. (including subser. lect. notes artif. intell. lect. notes bioinformatics)* (Vol. 9817 LNCS, pp. 175–190). doi: 10.1007/978-3-319-45507-5_12

Tosh, D. K., Vakilinia, I., Shetty, S., Sengupta, S., Kamhoua, C. A., Njilla, L., & Kwiat, K. (2017). Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance. In *Decis. game theory secur.* (pp. 519–532). Springer International Publishing.

Tumay, M. (2009). Asymmetric Information and Adverse Selection in Insurance Markets: The Problem of Moral Hazard. *Yönetim ve Ekon.*, *16*(1), 107–114.

Ulbinaite, A., Kucinskiene, M., & Le Moullec, Y. (2014). The complexity of the Insurance purchase decision making process. *Transform. Bus. Econ.*.

Van Eeten, M. (2017). Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity For Authors Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity. *Digit. Policy, Regul. Gov.*, *19*(6), 429–448. Retrieved from https://doi.org/10.1108/DPRG-05-2017-0029 doi: 10.1108/DPRG-05-2017-0029

Wagenaar, H. (2014). *Meaning in action: Interpretation and dialogue in policy*. Routledge.

Wagner, W. C. (2015). *Cyber Insurance: What do Cyber Insurance Policies Cover and Cost?* Retrieved from https://www.privacyanddatasecurityinsight.com/2015/04/cyber-insurance-what-do-cyber-insurance-policies-cover-and-cost/

Willig, C. (2008). Grounded theory methodology. In McGraw-Hill Education (Ed.), *Introd. qual. res. psychol.* (3rd ed., p. 248).

Wolff, J., & Lehr, W. (2018, mar). Roles for Policy-Makers in Emerging Cyber Insurance Industry Partnerships. *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract{_}id=3141409

Woods, D., Agrafiotis, I., Nurse, J. R., & Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *J. Internet Serv. Appl.*, *8*(1). doi: 10.1186/s13174-017-0059-y

Woon, I., Tan, G.-W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 Proc.*, 31.

Yang, Z., & Lui, J. C. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Perform. Eval.*, *74*, 1–17. doi: 10.1016/j.peva.2013.10.003

Zhang, H., Stanton, B., Li, X., Mao, R., Sun, Z., Kaljee, L., … Qu, M. (2004). Perceptions and attitudes regarding sex and condom use among Chinese college students: A qualitative study. *AIDS Behav.*. doi: 10.1023/B:AIBE.0000030242.46843.71

A

Actor analysis for getting cyber insurance

The following is the complete context diagram first presented in Chapter 3. All the interfaces and relations are presented, where straight lines indicate a direct relationship between actors, and dotted lines indicate informal relations between them. Finally, Table A.1 presents the list of stakeholders indicated in the context diagram.

- EO1: The insurance market is the primary beneficial actor of companies getting cyber insurance. Therefore they will try to influence the companies' mindset about the necessity of the product and its benefits.
- E02: Since the number of personnel SMEs can have is limited they tend to outsource activities for which they are not expert, or they do not have the people to carry them out. This is the case for IT security, SMEs rely on the advice and services these companies give.
- E03: Insurers have found support to provide cyber insurance in IT security companies. Some insurers provide services from these IT companies as part of the cyber insurance coverage like monitoring and support when a cyber attack occurs.
- E04: The insurance market has a direct influence on the cyber insurance as a product since the actors are the one developing and promoting the product. They represent the supply side.
- E05: Companies are the main buyer of cyber insurance. Regarding SMEs, they are usually first approached by a broker either directly or through a sectorial organization. Companies represent the demand side.
- E06: The role of the government has been studied to indirectly influence a more strength cyber insurance market (e.g. (Woods et al., 2017; Wolff & Lehr, 2018)). It is expected in the future to have a more direct influence.
- E07: IT security companies could have different interests in the existence of a cyber insurance market since they can provide their services to both supply and demand side.
- E08: The insurance market will try to influence the government through its different agencies to have a more active role in the adoption of cyber insurance. Companies lobbying with policymakers is a real scenario to achieve this goal.
- E09: Government can have direct influence on companies through regulations. Even that the influence is not currently linked with cyber insurance, it has to be recognized as a potential scenario in the future. Currently, the Dutch Data Protection Act is an example of the obligations companies have in case of data leakages.

- E10: IT security companies are important in this analysis in two ways. The first one, they can act as part of the cyber insurance product to enter in action when a cyber attack occurs. The second, they are commonly hired by SMEs to outsource their IT security services.

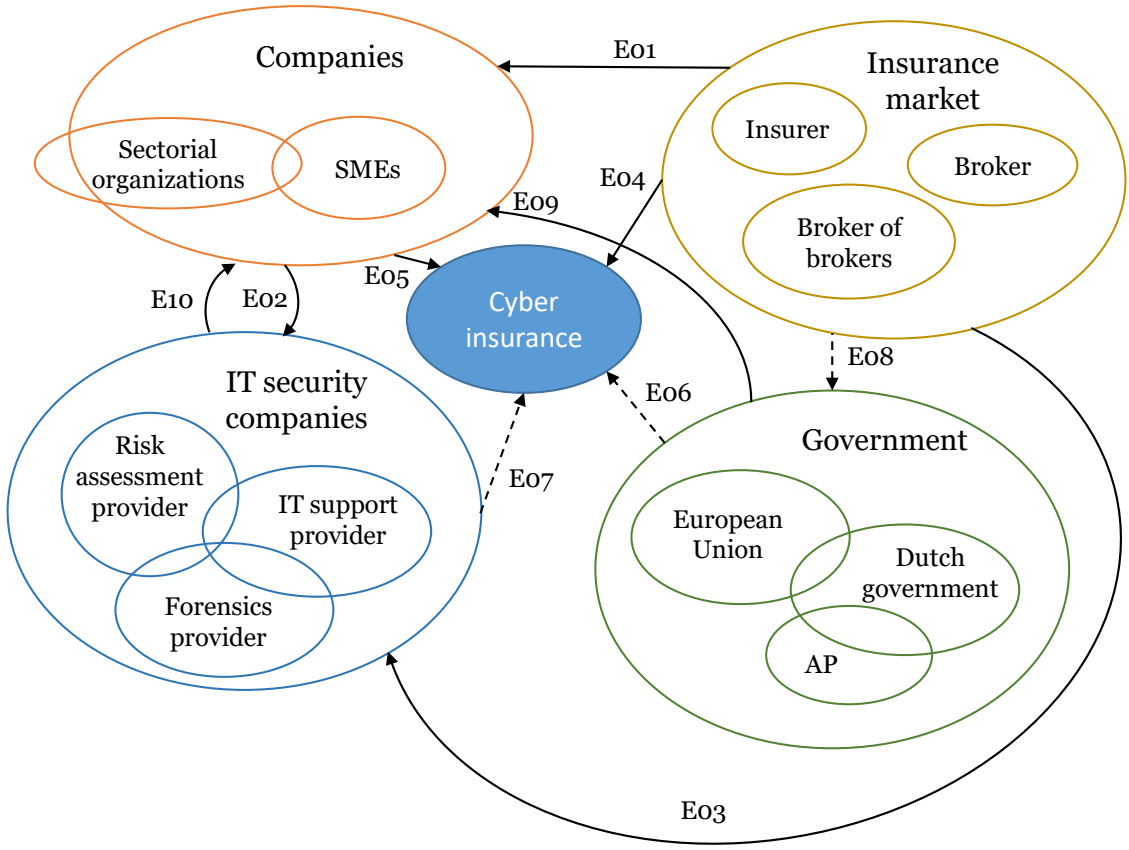


Figure A.1: Cyber insurance complete context diagram

Actor	Description	Source
Companies		
SMEs	The category of SMEs is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.	(European Union, 2003)
Sectorial organizations	Sectorial organizations represent the common interests of business that belong to a specific sector and provides a variety of services for its members.	(PUM Netherlands, n.d.)
Insurance market		
Insurer	The company helping their clients prevent cyber risks and mitigate their impact when they materialize.	(Insurance Europe, n.d.)
Broker	Is the intermediary between the company and the insurer. A broker can provide information about cyber insurance products from different insurers.	(Bonner, 2018)
Broker of brokers	Also known as Managing general agent, they act on behalf of different insurance companies to oversee their business in a particular area.	(Hager, 2016)
IT security companies		
Risk assessment provider	A company providing a company´s cyber security practices for risk transfer purposes. It reviews holistic threats to identify coverage applicant´s risk posture. This provider facilitates the insurance underwriting process.	(Financier Worldwide, 2015)
IT support provider	It usually refers to the third party hired by a company to provide IT hardware, software and professional services. SMEs typically outsources their IT services to this type of provider.	(Cox, 2017)
Forensics provider	A party in charge of analyzing if a data breach occurred, investigating the cause and scope of the breach.	(Wagner, 2015)
Government		
European Union	The economic and political union between 28 countries in Europe. In this definition are included the European Council, European Parliament and European Commission since these are the institutions in charge of the legislative processes.	(European Union, n.d.)
Dutch government	General representation of the Government of the Netherlands.	(Government of the Netherlands, n.d.)
AP	The Dutch organization in charge of supervising the compliance with laws regulating the use of personal data.	(Autoriteit Persoonsgegevens, n.d.)

Table A.1: List of stakeholders

B

Semi-structured interviews

The interviews with SME's representatives were conducted in a semi-structured way. This approach allowed to set predefined questions, primarily defined by the PMT elements and complemented by general questions and questions regarding the business process for cyber insurance adoption. The questions can be open, and the method allows flexibility regarding the order they are asked. In this section, the interview protocol that was used is presented. Then, the questions are separated per scenario according to Section 4.1. As mentioned in the methodology, all the interviews were transcribed, but the full transcripts are not included as part of the Appendix. The reason for this is to respect the confidentiality of the interviewees. Previous to the interviews, it was indicated to the interviewees that fragments of what they say could be used, but this is only done with the purpose to illustrate the results better. It is considered that having access to the full transcripts, even in a public version, does not provide additional value to the outcome of the results or the discussion.

Interview protocol

After one of the actors in Table 4.4 was able to provide contacts regarding SMEs that have been in the process for getting cyber insurance, the representative of the company was contacted by phone or email. Once the SME representative agreed on participating, a consent form was send in advanced to guarantee the anonymity of the interviewee and explain the research objectives for which the data will be used. Each interview started with the following introduction to present the research objectives:

> "Thank you for participating in this interview which has the purpose to study the decision-making process SMEs follow to acquire a cyber insurance with a perspective on what motivates them to protect themselves from cyber risks. I'm Inés Martínez, Master student at TU Delft. Cyber insurance is not a new concept, it has been in the market for more than two decades, nevertheless the level of adoption has been low, especially when comparing EU with US, where the latter counts for 90% of the market. Because of this, the aim of this study is to understand the reason of this trend.
>
> The interview will be recorded with the purpose of analyzing the data, and the only persons that will have access to it are the two main researchers. Any personal information that can identify you or your company will not be included, thus keeping the interview anonymous. It's also important to mention that there are no right or wrong answers. I understand that your time is extremely valuable, and I appreciate your effort in helping me in this important research effort."

Questionnaire

Table B.1 indicates the general questions made to SMEs' representatives. These questions were done at the beginning of the interview, and their main objective is to gather demographical data and know in general terms their opinion regarding cyber insurance. These questions also helped to set a relaxed mood at the beginning of the interview by making simple, straightforward questions.

General questions			
Scenario	**I. Have CI**	**II. Is considering CI**	**III. Don't have CI**
Questions to gather demographical data	In which sector does your organization belong (e.g.: financial, healthcare, industrial, technology, utilities)?		
	What is the number of employees working for the company?		
	What is your current position in the company?		
	Is there someone (or a certain department) in charge of security management? And if so, which role does it have or what department is it?		
General reasons about cyber insurance	Which are the main reasons for getting a cyber insurance?	Which are the main reasons for getting a cyber insurance?	Do you already have insurances like Errors & omissions (E&O) liability, commercial general liability or another similar? Do you think this product covers your concerns related to cyber security?

Table B.1: General questions for SMEs, per scenario

Next, Table B.2 presents the questions related to the business process. As it can be seen, Scenario III does not have any question. As shown in Chapter 3, in Figures 3.2.1 and 3.4, the steps by a company that decided not to get cyber insurance occur in an early stage. For companies in this scenario, it was decided to focus on the questions based on PMT to know their reasons for taking this decision.

Business process			
Scenario	**I. Have CI**	**II. Is considering CI**	**III. Don't have CI**
Business process	What kind of broker are you working with? - One with whom I have already worked with or not - A specialized broker or a broker focused on cyber security - A regional or global insurer/broker - Other		No question related
	Please describe the process for selecting and buying cyber insurance with your broker and insurer. Did you experience any problems? What did you like about the process?	Please describe the process for selecting cyber insurance with your broker and insurer. Have you experienced any problems? What have you liked about the process?	No question related
	How would you assess the success of the use of a cyber insurance?	No question related	

Table B.2: Business process related questions for SMEs, per scenario

Finally, Table B.3 shows the questions related to PMT. The questions are grouped per PMT element, and it has to be noted that PMT's components do not have an explicit question since the elements are the ones defining the components. Questions differ depending on the SMEs scenario they are situated.

Questionnaire for SMEs per scenario			
PMT concept	**I. Have CI**	**II. Is considering CI**	**III. Don't have CI**
Sources of information	**No question**		
Intrapersonal	Does your role in the company is related with keeping the company secure from cyber threats? How did you first hear about cyber insurance? Do you know companies who already have a cyber insurance?		
Environmental	Have you discussed the cyber insurance topic with your clients or other companies? If yes, what was their opinion about cyber insurance? Do you personally know a company that has suffered a cyber attack?		
Threat appraisal	**No question**		
Vulnerability	What factors make or could make the company more susceptible to security attacks? Meaning, what makes your company easily affected by attackers?		
	Do you have alternative protective measures besides cyber insurance?		What protective measures do you have against these security attacks or threats?
Severity	What are the main security threats for which you wanted to get a cyber insurance?	What are the main security threats for which you would get a cyber insurance?	What are the main security threats you consider relevant to the company?
	Do you think some of them have more impact than others?		
Rewards	Is any of the next reasons a potential cause for you to not select a cyber insurance? - Do not get a cyber insurance until other companies do so. - There are no sanctions for not having a cyber insurance. - Do not buy cyber insurance to save budget. - It is not included in the security guidelines of the company. - You think it is not necessary. Can you think of any additional reason?		
Coping appraisal	**No question**		
Response efficacy	Did the insurer request to implement certain/additional security controls?	Has the insurer requested to implement certain/additional security controls?	Do you think there are additional security controls needed to be implemented to deal with cyber risks?
	What are your current expectations with your cyber insurance policy?	What expectations do you have if you decide to get a cyber insurance?	No question related
Self-efficacy	Have you experienced a cyber attack? How did you deal with it?		
	Did you have to fill a claim?	No question related	
	Do you fully understand the coverage provided by your cyber insurance and in which cases you would be able to use it?	Do you fully understand the coverage offered by your cyber insurance and in which cases you would be able to use it?	No question related
	No question related		Do you believe to have a good security management strategy?
	No question related		What would motivate you to engage in acquiring a cyber insurance?
Response cost	What potential drawbacks would you associate with adopting a cyber insurance?		No question related
	What do you think about the premium price?		

Table B.3: Questionnaire for SMEs per scenario

C

List of codes and group codes

Code	Grounded	Code Groups	Grounded per group
Asset: Company's reputation	21	CI adoption	137
CI adoption: Benefits: Stress reduction	2	CI adoption	
CI adoption: Benefits	4	CI adoption	
CI adoption: Drawback	2	CI adoption	
CI adoption: Driver	52	CI adoption	
CI adoption: Driver: Added value	4	CI adoption	
CI adoption: Impediments	25	CI adoption	
CI adoption: Impediments: CI is not necessary	7	CI adoption	
CI adoption: Impediments: No added value	4	CI adoption	
CI adoption: Impediments: Silent coverage	5	CI adoption	
CI adoption: Just in case	1	CI adoption	
CI adoption: special coverage	1	CI adoption	
Additional services: Incident response management	9	CI adoption	
CI process	31	CI process	89
Ci process: Additional information requested	1	CI process	
CI process: Business contract	37	CI process	
CI process: CI form	2	CI process	
CI process: Flexibility	2	CI process	
CI process: Negotiation with managers	3	CI process	
CI process: Responsible for security/safety/insurance	8	CI process	
CI product research	5	CI process	
Company type: Entrepreneur	1	Company type	16
Company type: Nonprofit organization	1	Company type	
Company type: Small company	14	Company type	
Additional services: Incident response management	9	Cyber insurance	
Additional services: PR support	3	Cyber insurance	29
CI: Claim	2	Cyber insurance	
CI: Expectations	13	Cyber insurance	
CI: Expectations: Work as promised	2	Cyber insurance	
Cyber security: External cyber security provider	21	Cyber security	82
Cyber security: Incident internal handling	4	Cyber security	
Cyber security: Internal security expertise	9	Cyber security	
Cyber security: Keep investing in cyber security	13	Cyber security	
Cyber security: Knowledge	16	Cyber security	

Cyber security: No cyber incident experience	10	Cyber security	
Cyber security: Point of improvement in security	3	Cyber security	
Cyber security: Security audit	2	Cyber security	
Cyber security: Security risk assessment	4	Cyber security	
Cybersec incident	12	Cyber security incident	20
Cybersec incident: Consequence	8	Cyber security incident	
Information source: Cyber attacks in the media	9	Information source	63
Information source: External discussion	4	Information source	
Information source: External experience	17	Information source	
Information source: External sources of information	10	Information source	
Information source: Knowledge (by insurer/broker)	12	Information source	
Information source: Knowledge sharing	6	Information source	
Information source: Previous experience	5	Information source	
[PMT] Coping appraisal	99	PMT	700
[PMT] Environmental	30	PMT	
[PMT] Intrapersonal	32	PMT	
[PMT] Response cost	24	PMT	
[PMT] Response efficacy	35	PMT	
[PMT] Rewards	39	PMT	
[PMT] Self-efficacy	42	PMT	
[PMT] Severity	29	PMT	
[PMT] Sources of information	62	PMT	
[PMT] Threat appraisal	187	PMT	
[PMT] Vulnerability	121	PMT	
Policy: Additional policy requirements	8	Policy	36
Policy: Clear coverage	9	Policy	
Policy: Coverage	9	Policy	
Policy: Damage coverage	7	Policy	
Policy: Unclear coverage	3	Policy	
Premium: Fair	6	Premium	42
Premium: High price	5	Premium	
Premium: Low price	2	Premium	
Premiums: Price	26	Premium	
Premiums: Price goes down	3	Premium	
Regulation: Fines	1	Regulations	16
Regulation: GDPR	8	Regulations	
Regulation: New regulations	3	Regulations	
Regulation: Sectorial regulator recommendations	4	Regulations	

Risk transfer	11	Risk	98
Risk: Acceptable risk	11	Risk	
Risk: Attacker motivation	14	Risk	
Risk: Dynamic risk	3	Risk	
Risk: Economic motivation	7	Risk	
Risk: Inaccurate perception	4	Risk	
Risk: Low probability	6	Risk	
Risk: Perceived exposure to risks	26	Risk	
Risk: Unacceptable risk	7	Risk	
Risk: Uninsurable risk	9	Risk	
SC: Access control	6	Security controls	126
SC: Alternative protective measures	49	Security controls	
SC: Antivirus	3	Security controls	
SC: Backup	2	Security controls	
SC: Business contingency plan	11	Security controls	
SC: BYOD policy	1	Security controls	
SC: Data protection	5	Security controls	
SC: Encryption	3	Security controls	
SC: Firewall	5	Security controls	
SC: Monitoring system	2	Security controls	
SC: Offline workflow	1	Security controls	
SC: Pentesting	2	Security controls	
SC: Redundancy	4	Security controls	
SC: Secure data sharing	5	Security controls	
SC: Security controls from insurer	2	Security controls	
SC: Security management strategy	17	Security controls	
SC: Security training	5	Security controls	
SC: Serious security games	1	Security controls	
SC: SLA	1	Security controls	
SC: Social monitoring	1	Security controls	
Sec. goal: Awareness	28	Security goal	42
Sec. goal: Preparedness	1	Security goal	
Sec. goal: Reliability	6	Security goal	
Sec. goal: Resilience	6	Security goal	
Sec. goal: Stronger protection	1	Security goal	
Thrat: Physical	1	Threat	77
Threat: Blackmail	1	Threat	
Threat: Commoditised attacks	3	Threat	
Threat: Cyber criminals	4	Threat	
Threat: Data leakage	12	Threat	
Threat: Data loss	5	Threat	
Threat: Disgruntled employee	1	Threat	
Threat: Espionage	6	Threat	
Threat: Financial fraud	2	Threat	
Threat: High impact	2	Threat	
Threat: IP loss	2	Threat	
Threat: Moral hazard	1	Threat	
Threat: Nation-state actor	3	Threat	
Threat: origin of impact	1	Threat	

Threat: Phishing	8	Threat	
Threat: PII	3	Threat	
Threat: Ransomware	7	Threat	
Threat: Service disruption	9	Threat	
Threat: Unauthorized access	6	Threat	
Vulnerability: Cloud technology	13	Vulnerability	35
Vulnerability: Digital communication	9	Vulnerability	
Vulnerability: Human errors	2	Vulnerability	
Vulnerability: Interdependent security	5	Vulnerability	
Vulnerability: Legacy	2	Vulnerability	
Vulnerability: Low awareness	3	Vulnerability	
Vulnerability: Low preparedeness	1	Vulnerability	
[Other] Interesting	1		
Asset: Valuable information	4		
Bad experience	3		
Changes in behavior	4		
CI adoption: Customer pressure	4		
CI: unskillful insurer	3		
Cost-benefit analysis	2		
Cyber insurance market	5		
Cyber insurance provider	1		
Different insurer	1		
Extra question	9		
Former insurer	8		
Geographical coverage	3		
Insurance type: Car insurance	1		
Insurance type: Fire insurance	2		
International safety/security standards	4		
IT manager	1		
Lack of CI products	1		
Lawyers	3		
Liability	9		
Negative	20		
Neutral	11		
New product	5		
Not interesting to hack	4		
Open data	2		
Optional insurance	1		
Other companies with CI	2		
Positive	5		
Significant cyber incident	1		
Similar insurance	14		
SME behavior	2		
Supply chain	13		

Table C.1: List of codes and group codes generated in Atlas.ti