Cyber insurance adoption among Dutch SMEs. An on-field study based on PMT

Inés Martínez
Faculty of Technology, Policy and Management
Delft University of Technology
I.MartinezBustamante@student.tudelft.nl

***Abstract*—Cyber security is getting more attention in the last decades. Unfortunately, the 100% cyber security protection is impractical and impossible, and therefore, we need to consider other cyber risk management strategies. One of them is cyber insurance, but its adoption has been slowly in Europe and even more among SMEs. This paper presents a qualitative study based on empirical data collection about the SMEs decision-making process to adopt cyber insurance. PMT is used as an underlying theory to build the interview questionnaire. The results show the different elements that makes a company select this product or reject it.**

***Index Terms*—cyber security, cyber risk, cyber insurance, qualitative study, Protection Motivation Theory, decision-making.**

I. Introduction

It only takes a look at the news to realize that cyber attacks are a potential threat to different types of industries and their users. 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 [1]; the multinational bank J.P. Morgan Chase & Co. suffered an intrusion compromising the data of 7 million small business and 76 million households [2]; and Equifax, one of the worlds three largest consumer credit bureau, suffered the loss of 145.5 million U.S. citizens' sensitive data, along with users data from Canada and the United Kingdom [3]. Nowadays, 130 security breaches on average per year worldwide [4] are happening, and cyber security breach may stay undiscovered for more than 200 days [5]. Protective measures like security awareness, intrusion detection systems, and 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.

There are five main types of risk mitigation strategies: 1) accept, 2) avoid, 3) mitigate, 4) share, and 5) transfer. [6]. Since it is not possible to fully protect the companys systems, the right mix of the risk management strategies is of great importance for any company using information technologies (IT). The insurance industry comes into play as part of the risk transfer strategy, with cyber insurance 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. The OECD identifies cyber insurance as a type of risk of highest concern to doing business [7]. 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. While the promise of cyber insurance is high, adoption rates have fallen short of expectations, especially for Europe. For instance, a survey from CIAB shows that only 32% of companies in the U.S. purchased some form of cyber liability [8], and the U.S. is the most developed market by having 90% of the global cyber insurance market, while Europe counts for 9% [7].

The cost of cyber crime varies per type of organization. The Ponemon Institute [4] has found differences depending on the organizations' size, industry sector, and even country. Regarding organizations 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.

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, a different approach to understanding the reasons for the low rate among SMEs on getting cyber insurance should be taken. The traditional way has followed the use of quantitative and mathematical models (e.g., [9]–[11], but these solutions cannot solve the behavioral causes. One way to look at this problem is by analyzing the way individuals make decisions when purchasing a product, like 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.

This research focuses on the elements defined in PMT such

as: intrapersonal and environmental sources of information, vulnerability, severity, rewards, response efficacy, self-efficay and response costs, to find the reasons companies have regarding cyber insurance adoption. The scope is in the Netherlands and specifically in Small and Medium Enterprises (SMEs). The research question to be answered is:

How can PMT explain the reasons for cyber insurance adoption among Dutch SMEs?

The paper is organized as follows: section II explains PMT's theoretical foundation. Next, in section III we discuss the approach to examine SMEs' perceptions about cyber insurance based on PMT's elements, which is done through a series of interviews to SME's representatives involved in the decision-making process to get cyber insurance. Section IV shows the results focusing on the impact PMT elements have on the final decision companies make. The results are discussed in Section V together with the contribution and advice for future research. Finally, Section VI provides a conclusion.

II. Protection Motivation Theory for cyber insurance

There are different behavioral theories like Theory of planned behavior [12] to predict and explain human behavior where the central factor is the intention to perform a certain behavior; technology acceptance model to explain the perceived usefulness and ease of use in the intention to use a system; and protection motivation theory where the perception of a fear initiates a cognitive appraisal process where the outcome is the protection motivation measure. 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., [13] and [7]). These characteristics make PMT suitable to analyze the decision-making process to select cyber insurance

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) [14]. PMT links these two aspects to antecedent communication stimuli and 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).

Figure 1 displays PMT model. The fear of a company being affected by a cyber-attack should first exist to consider potential solutions to protect against it. Previous research in the information security field about the use of PMT model [15]–[17] gives a background to explain the protective process individuals follow when they believe themselves or their organizations are susceptible to security threats.

To show the relation of PMT in the cyber insurance context, the definition of PMT elements are adapted to provide examples in the cyber insurance case. A detailed definition of the elements can be found in [18], [19]. The output will later be used to develop 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. The two factors comprising this component in the cyber security 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 the news reports), or a company adopting cyber insurance after directly witnessing a cyber attack.
  - ***Intrapersonal sources of information***: personality aspects like the professional background, role in the company and knowledge about cyber security; feedback from prior a experience like directly witnessing a cyber-attack.
- ***Threat appraisal.*** The component that evaluates the maladaptive behavior is composed of the next elements:
  - ***Vulnerability***: the probability that a company will experience harm, therefore, if the company believes its susceptible to suffer a cyber attack at all, maybe because company activities are of interest for attackers or because they have taken precautionary measures with its IT security.
  - ***Threat severity***: the degree of harm from the unhealthy behavior, therefore, if a company thinks is susceptible to be attacked we need to know the attacks they are more afraid of having and how severe would the consequences be.
  - ***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 (for not having cyber insurance); intrinsic rewards like the belief that is not a useful measure because the likelihood of having a cyber-attack is low, because the measure is not included in the company guidelines, or to project an image that the company is capable of protecting by itself.
- ***Coping appraisal.*** The component that evaluates the ability to cope with and avert the threatened danger is composed of the next elements:
  - ***Response efficacy***: this is the belief by the company that adopting a response in the form of cyber insurance will work, this can be translated as the expecta-

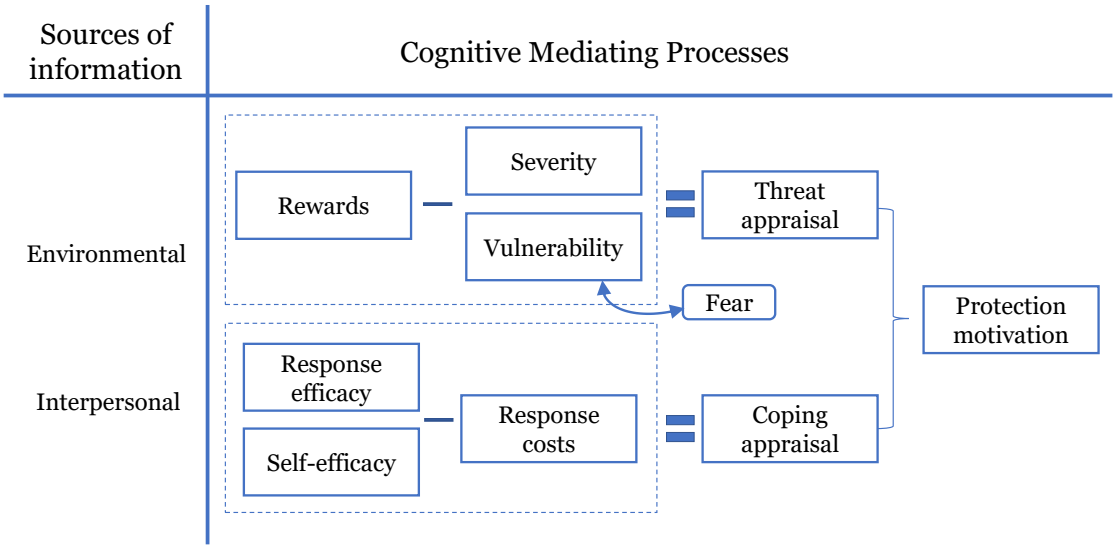

Fig. 1. Roger's protection motivation theory model

tions the company has about how the insurance will work as well as the support by the insurer or broker.

- ***Self-efficacy***: the perceived ability of the person to carry out the adaptive response, like, how much the person knows about the cases when the cyber insurance can be used or how able the company has been by dealing with a cyber-attack.
- ***Response costs***: any costs associated with getting cyber insurance. The first cost to consider is the financial cost, meaning the premium price, but also any negative effect that could come out from the acquisition of the product, 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.

III. Research Method

This research followed a qualitative approach based on literature review and empirical data collection supported by semi-grounded theory techniques, such as coding of interview transcripts and code classification. 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.

As a research method, we choose a qualitative approach, with a series of semi-structured interviews with SMEs' representatives. To analyze collected data and build a theoretical model of drivers and impediments for cyber insurance adoption based on PMT elements, we use following techniques from semi-grounded theory approach: coding of interviews transcripts and code classification.

PMT is a theory that can be applied to research in different ways, being the quantitative approach the most used (e.g., [20]–[23]). The work done by Zhang [24] and Posey [25] are examples of the use of PMT for qualitative research, which provides guidelines on how to design the semi-structured interviews using PMT. The questions related to PMT concepts create a match between this theory and the cyber insurance acquisition reasoning.

An SME could experience three phases when getting cyber insurance, then three different questionnaires are necessary. The full questionnaires can be found in the Appendix. The three phases or scenarios an SME could experience are:

label=*

1) Company has cyber insurance
2) Company is considering getting cyber insurance
3) Company decided not to get cyber insurance

The first approach to get in contact with SMEs is through brokers or insurers, but since brokers can represent several insurers at the same time this seemed to be a more natural path to broaden the possibilities. An alternative to the broker are the Sectorial organizations since they represent the companies' interests of a specific sector and all of them are gathered in one place. Without exception, every actor we had a discussion with to approach SMEs to interview, expressed concern and hesitation about the willingness of companies to participate. Additionally, the research occurred near the summer holiday period, which was also a factor that reduced the level of participation. After talking with the brokers and sectorial organizations and explain the research, they would contact their clients and ask if they were willing to be interviewed. Then, they would provide us with the SMEs' representative contact, and the main researcher contacted them to set the date and time for the interview. In the end, 17 SMEs contacts were gathered, and 11 companies agreed to participate in the interview. All the companies received the consent form in advance of the interview to explain the research objectives

for which the data will be used and guarantee the anonymity of the interviewee. Of the 6 companies that did not participate, their main reasons were that they wanted the interview in Dutch or they were short on time. For the first reason, 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. For the second reason, it is a reflection of the SMEs situation about their resources limitation. The interviews started formally on May 31st and ended on July 19th. Table I summarizes the interviewees by sector, SME type, security management situation, scenario (according to section the previous paragraph), 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. 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 at the moment of the interview. If the sample size had increased to over 15 interviews, I04 would have been dismissed, but unfortunately this did not happen.

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 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. After the open coding is done for all the interviews, group codes are created. These are based on relevant themes related with answering the sub-research questions. Example of these themes 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.

IV. Results

The results generated from the analysis of the transcribed interviews through the use of semi-grounded techniques are shown per PMT concept: sources of information, threat appraisal and coping appraisal.

A. Sources of information

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 discussed, it was requested that the representative should be involved in the process for selecting 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

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

TABLE I
DEMOGRAPHICAL DATA ABOUT SMES INTERVIEWED

Company	Sector	SME type[1]	Someone in charge for security management?	Scenario	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 [26]

TABLE II
RESUME OF ANSWERS FOR PMT'S SOURCES OF INFORMATION COMPONENT

PMT element	Question	Summary of answers
Intrapersonal	Role in the company related with keeping the company secure?	Yes
	First approach to CI*?	7 out of 11, Broker
	Know other companies with CI?	2 out of 11, yes
Environmental	Discussed CI with companies?	1 out of 2, yes
	Know companies that suffered a cyber attack?	5 out of 11, yes

* CI - Cyber insurance

discussing a topic with an external party and the next feature regarding their knowledge about other companies suffering a cyber attack, are related to the ***environmental*** element. For the latter, the 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.

Table II shows a resume of the answers provided for the PMT component sources of information.

B. Threat appraisal

TABLE III
RESUME OF ANSWERS FOR PMT'S THREAT APPRAISAL COMPONENT

PMT element	Question	Summary of answers
Vulnerability	What factors make the company vulnerable?	Digitalization Confidential information Reputation
	What protective measures does the company have?	Firewall I&A management Business contingency plan
Severity	What are the main security threats?	Data leakage Service disruption Phishing
Rewards	Why would you not get a CI?	Price Not necessary Unclear policy

The element **vulnerability** analyses the main reasons for companies to perceive a degree of probability that they could experience a cyber attack. The most cited reason is *digitalization*. Below some of the answers:

> *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 dont 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 this aspect, 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: interdependency with other companies, criminals (national and international), money, lack of specialists, internal IT and security services, disgruntled ex-employee, legacy systems, lack of awareness, human errors, being part of the financial sector, espionage, and having customers with high revenue.

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 I. 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.

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 [4] 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*. 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 dont recognize at first sight, we had to transfer the money and then we realize that those email addresses dont match.* ***(I07)***

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.

Overall, the most mentioned answers besides *firewall* were related with *identity and access management* to company's data and the implementation of *business contingency plans*.

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)***

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)***

Table III shows a resume of the answers provided for the PMT component sources of information.

C. Coping appraisal

TABLE IV
RESUME OF ANSWERS FOR PMT'S COPING APPRAISAL COMPONENT

PMT element	Question	Summary of answers
Response efficacy	Additional security controls besides CI?	No
	Additional security controls for the company?	No
	Expectations with CI?	Help during the process Will not have to use it
Self-efficacy	Have you experienced cyber attack before having CI?	3 out of 11, yes
	Have you experienced cyber attack after having CI?	No
	Is CI policy understandable?	Yes
	Do you have a good security management? (Scenario III)	Yes
	Reasons to engage acquiring a CI?	No added value Customer pressure
Response cost	Premium price?	Fair

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. For the five 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)***

Regarding the expectations for cyber insurance, six companies provided 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.

- 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.

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 thats already in our business contingency plan. Thats why we dont need the insurance.* ***(I04)***
> *I dont see any reason. Reputation risk cant 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. 4 out of 11 companies said it is a fair price, two companies mentioned it is cheap, four companies do not have and opinion about the price, and one mentioned considers the premium price to be high.

Table III shows a resume of the answers provided for the PMT component sources of information.

V. Discussion

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. As recent research from KPMG shows [27], commoditized attacks are growing and even if they do not have significant financial impacts as high-end attacks, they can be easily spread and affect more persons or companies. Additionally, [28] points out that SMEs are the target of almost half of cyber attacks.

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.

For the **sources of information** component, it was found that cyber insurance is a new concept among SMEs and this has lead insurance companies to take a proactive role and create awareness about cyber risks before starting to offer the product. Also, during the process to get the interviews it was found that companies do not feel comfortable talking about cyber threats and the way to deal with them. This was one of the reasons for not getting as much as interviews as desired and it is also related to the fact that companies do not communicate between each other their actions related to cyber security.

For the **threat appraisal** component it was found that digitalization, having the client's confidential information, and reputation is what SMEs are most fear of losing since that would have a direct effect on the trust their clients have on them. Digitalization of their information is necessary to grow in the business, but at the same time is the main factor that makes them vulnerable to being attacked. Because of the increase in the digital information they have, technical protective measures are of great concern to keep them safe. These reasons together with the low probability of experiencing a cyber attack make the companies start to consider if cyber insurance could be a response as a risk transfer strategy.

Regarding the **coping appraisal** component, cyber insurance seems to be an attractive proposition to transfer the risk of potential losses in case of a cyber attack since the insurance policy is understandable and the premium price is fair. Moreover, cyber insurance provides complementary knowledge about how to deal with a cyber attack, something SMEs value since they usually do not have the personnel with the experience to deal with these kinds of situations. On the contrary, if the SME do have the personnel with experience in information security and have invested enough money in protective measures to prevent themselves from cyber attack and be resilient, their reasons to get cyber insurance are reduced.

A. Contribution and future research

Cyber insurance adoption is both a technical and a behavioral matter, but since to the day is impossible to be fully protected against cyber attacks concerning the technical measures, behavioral elements were analyzed in this paper. Research based on PMT to study cyber insurance has not been done to the extent knowledge of the researchers. A theory like PMT was used to gather empirical data from the interviews with the SME's representatives in the decision-making process for cyber insurance. The main contribution of PMT was on helping to develop the relevant questions in the cyber insurance context.

Different actors can be benefited from this study. The supply side of the market, represented mainly by insurers and brokers, can sense the high expectations companies have on the product. Therefore they should have all the necessary measures in place to comply as indicated in the policy. They should continue with good practices like first creating awareness among the companies before starting to sell the insurance, show the historical drop of the premium price, and invite companies to forums where other companies can expose their case if they have suffered a cyber attack. Close experience with cyber attacks raises the level of awareness.

For the demand side, the Dutch SMEs, they can identify elements to consider when evaluating the possibility to get cyber insurance and make their decision based on a holistic and well-informed approach, avoiding with this, making decisions only based on fear or stressful circumstances. Moreover, keep a reasonable level of communication with the broker, especially if previous insurances have been in charge of that party. Finally, if IT services are outsourced, procure having it with companies with expertise in cyber security, and regular checks like penetration tests are included.

Regarding the future research, these findings should be contrasted with interviews to more SMEs in different sectors. A bigger number of participants is ideal but due to time constraints, reluctance from some companies and the summer holiday period, it was not possible to be achieved. 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.

VI. Conclusion

PMT has proved to be an interesting approach to understand the aspects influencing companies' decision regarding the selection of a product like cyber insurance. Through the separation of the threat appraisal and coping appraisal processes, different elements that makes a company feel threatened to then analyze the possible ways to deal with the threat are recognized. The understanding of PMT helped to develop the three different questionnaires made to SMEs' representatives. These questionnaires were similar and only adapted depending on the scenario the company is. Through the development of the interviews, it was recognized that the way SMEs analyze their decision to get or not cyber insurance goes in accordance with the processes stated in PMT, which is evaluating not only personal experience but also the surroundings. Companies first perceive their level of exposure to risk and the level of their protective measures to determine the probability of an attack to occur. Then, if cyber insurance is a viable option, they will analyze the policy coverage and determine if the product provides additional services and value for the company. Price is always important as part of their decision.

References

[1] S. Fisher, "How to Calculate the Cost of a Target Breach At Your Company," 2014. [Online]. Available: https://www.laserfiche.com/simplicity/how-calculate-cost-target-breach-your-company/

[2] Fox, "JPMorgan data breach adds to concern over security of consumer data at banks, retailersle," 2016. [Online]. Available: https://www.foxbusiness.com/features/jpmorgan-data-breach-adds-to-concern-over-security-of-consumer-data-at-banks-retailers

[3] R. Hackett, "Equifax Breach Affects 2.5 Million More People Than First Reported," 2017. [Online]. Available: http://fortune.com/2017/10/02/equifax-credit-breach-total/

[4] Ponemon Institute, "2017 Cost of cyber crime study. Insights on the security investments that make a difference," Ponemon Institute LLC, Tech. Rep., 2017. [Online]. Available: https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

[5] P. Institute, "2017 cost of data breach study: Global overview," June 2017.

[6] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Risk management guide for information technology systems," 2002.

[7] OECD, "Enhancing the Role of Insurance in Cyber Risk Management," OECD, Tech. Rep., 2017. [Online]. Available: http://www.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en

[8] CIAB, "Cyber insurance market watch survey," May 2017.

[9] Y. Hayel and Q. Zhu, "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, 2015, pp. 22–34.

[10] D. K. Tosh, I. Vakilinia, S. Shetty, S. Sengupta, C. A. Kamhoua, L. Njilla, and K. Kwiat, "Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance," in *Decis. Game Theory Secur.* Springer International Publishing, 2017, pp. 519–532.

[11] Z. Yang and J. C. Lui, "Security adoption and influence of cyber-insurance markets in heterogeneous networks," *Perform. Eval.*, vol. 74, pp. 1–17, 2014.

[12] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, 1991.

[13] P. H. Meland, I. A. Tøndel, M. Moe, and F. Seehusen, "Facing uncertainty in cyber insurance policies," in *International Workshop on Security and Trust Management*. Springer, 2017, pp. 89–100.

[14] H. Leventhal, "Findings and Theory in the Study of Fear Communications," *Adv. Exp. Soc. Psychol.*, vol. 5, no. C, pp. 119–186, 1970.

[15] A. Gurung, X. Luo, and Q. Liao, "Consumer motivations in taking action against spyware: An empirical investigation," pp. 276–289, 2009.

[16] Y. Lee and K. R. Larsen, "Threat or coping appraisal: Determinants of SMB executives decision to adopt anti-malware software," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 177–187, 2009.

[17] I. Woon, G.-W. Tan, and R. Low, "A protection motivation theory approach to home wireless security," *ICIS 2005 Proc.*, p. 31, 2005.

[18] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory," *J. Appl. Soc. Psychol.*, vol. 30, no. 2, pp. 407–429, 2000.

[19] A. C. Clubb and J. C. Hinkle, "Protection motivation theory as a theoretical framework for understanding the use of protective measures." *Crim. Justice Stud. A Crit. J. Crime, Law Soc.*, vol. 28, no. 3, pp. 336–355, 2015. [Online]. Available: http://dx.doi.org/10.1080/1478601X.2015.1050590

[20] A. Reynaud, C. Aubert, and M. H. Nguyen, "Living with floods: Protective behaviours and risk perception of vietnamese households," *Geneva Pap. Risk Insur. Issues Pract.*, 2013.

[21] T. Grothmann and F. Reusswig, "People at risk of flooding: Why some residents take precautionary action while others do not," *Nat. Hazards*, 2006.

[22] K. Glenk and A. Fischer, "Insurance, prevention or just wait and see? Public preferences for water management strategies in the context of climate change," *Ecol. Econ.*, 2010.

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

[24] H. Zhang, B. Stanton, X. Li, R. Mao, Z. Sun, L. Kaljee, M. Clemens, S. Ravendhran, and M. Qu, "Perceptions and attitudes regarding sex and condom use among Chinese college students: A qualitative study," *AIDS Behav.*, 2004.

[25] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," *Inf. Manag.*, 2014.

[26] European Commission, "What is an SME? - European Commission." [Online]. Available: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

[27] Lloyd's, "Closing the gap. Insuring your business against evolving cyber threats," 2017.

[28] Independent.ie, "Cyber security: Half of all attacks are against small businesses and most not reported to gardai," 2018. [Online]. Available: https://www.independent.ie/business/dublin-information-sec/cyber-security-half-of-all-attacks-are-against-small-businesses-and-most-not-reported-to-gardai-37007405.html

Appendix
Questionnaire to SMEs

Figure 2 shows the questions made during the semi-structured interviews to SMEs' representatives. The questions are grouped per PMT element and it has to be noted that PMT's components do not have a explicit question since

the elements are the ones that define them. Questions differ depending the SMEs scenario which can be:

1) Company has a cyber insurance
2) Company is considering getting a cyber insurance
3) Company decided not to get a cyber insurance

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?		

Fig. 2. Questionnaire for SMEs per scenario