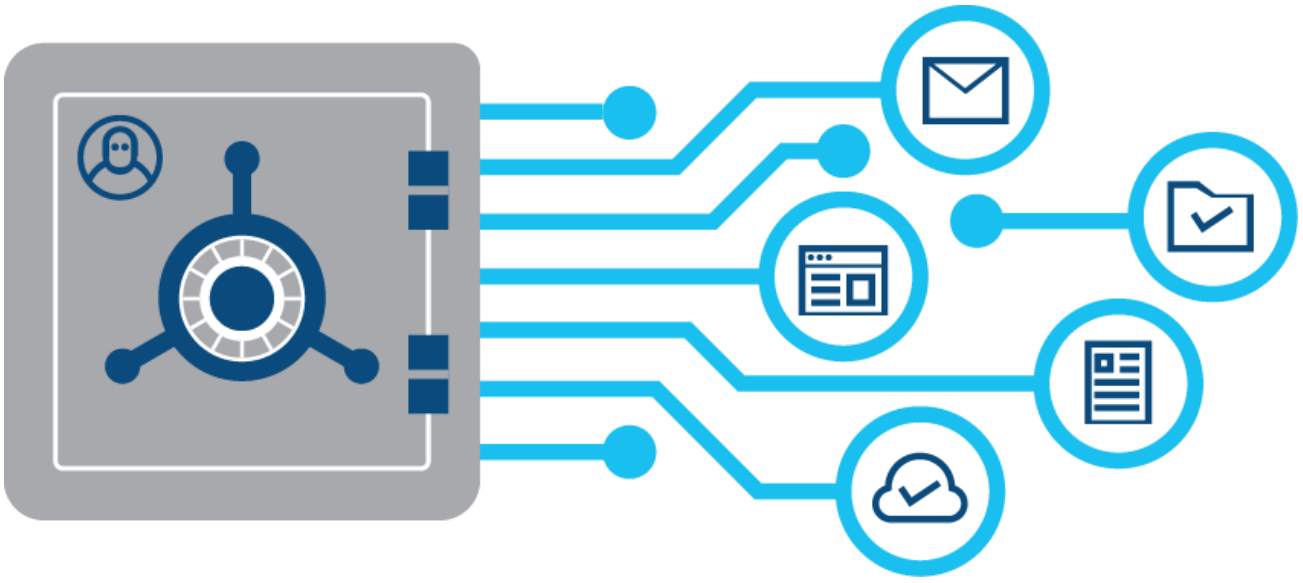
TILBURG UNIVERSITY

How Cyber Insurance Policies influence Cyber Security Levels



A. J. C. Muller

Bachelor Thesis IT & Management

Tilburg School of Economics and Management

Tilburg University

Student Information

Name: A. J. C. Muller
ANR: 856374
U-number: 1263981

Supervisor

Prof. Dr. M. Smits

Thesis

Title: “How cyber insurance influences cyber security levels”
School: Tilburg School of Economics and Management (TiSEM)
Department: IT and Management
Delivery date:: 10 - 12 - 2018
Type: Literature review
Word count: 7779

There are only two types of companies,

those that have been hacked,

and those that will be.

Robert Meuller

FBI Director, 2012

Abstract

This research focussed on the knowledge gap, which exists on the influence of policy within cyber insurance on the decision to implement cyber security measures. In order to fill this gap, this research has conducted a literature research, gathering known theories, methods, case studies, conclusions and recommendations from previous research. In order to establish a complete view of the variables and their interdependence, this research has studied the implementation of policies, contracts and requirements within cyber insurance as well as the cyber security level, how to measure cyber security levels and their influence on the decision to implement cyber security measures. This literature review has found that cyber insurance policies can positively influence the decision to implement cyber security measures. However, this influence is negatively affected by the cyber security level of the insured, which also negatively influences the decision to implement measures of cyber security. Furthermore, this literature review provides implications for future research into setting differentiated premiums and advises to gather actuarial data on cyber attacks, it also offers recommendations to cyber insurance companies for differentiating premiums based on cyber security levels.

Bachelor Thesis

1. Introduction into Cyber Attacks, Cyber Security and Cyber Insurance

1.1. Problem statement

Cisco (2018) explains that "A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim's network." Within the Annual Cybersecurity Report conducted by Cisco (2018), it was found that "the total volume of events has increased almost fourfold between January 2016 and October 2017". Even though the threats of such attacks are widely recognised, there is inadequate action being taken to defend companies in order to prevent these attacks from happening. (Ministry of Justice and Security, 2018). "Organisations are being successfully attacked using simple methods. As the recent period has shown, incidents could have been prevented and damage mitigated with basic measures" (Ministry of Justice and Security, 2018). Higher investments should be made by companies into cyber security in order to prevent cyber attacks, such as the attacks from January 2018 on major Dutch banks (Mather, 2018).

Solms and Niekerk (2018) describe cyber security as not being limited to the protection of the cyberspace itself but also including the protection of those whom function within the cyberspace and any of their assets which can be targeted through the cyberspace. Through cyber security companies can protect themselves from cyber attacks directed at the company. However, as the Dutch ministry of Justice and Security (2018) indicates, not enough measures are being taken by companies and this needs to be stimulated in order for companies to sufficiently protect themselves.

Cyber insurance is viewed upon as a possible way to incentive companies towards a higher investment in cyber security and self-protection against cyber attacks. According to research, conducted by Kesan, Marjuca and Yursic in 2014, solving certain challenges within the cyber insurance market will lead to several benefits. Amongst the benefits proposed by Kesan et al. 2014, is that of higher investments by companies in cyber security also resulting increasing levels of safety for information technology infrastructure.

1.1.1. Managerial and practical relevance

Cyber insurance provides a promising possibility to manage risk mitigate security problems:

> As an orthogonal approach to mitigating security problems, some have pursued the use of cyber-insurance as a suitable risk management technique. Such an approach has the potential to jointly align with the incentives of security vendors (e.g., Symantec, Microsoft, etc.), cyber-insurers (e.g., ISPs, cloud providers, security vendors, etc.), regulatory agencies (e.g., government), and network users (individuals and organizations), in turn paving the way for comprehensive and robust cyber-security mechanisms". (Pal, Golubchik, Psounis, & Hui, 2014)

In line with this statement, the market of cyber insurance in growing rapidly over the past few years. In 2016, 47.5% of the responding organisations on a cyber insurance survey (Kappelman,

2017) were making use of cyber-insurance and in 2017 this percentage has grown to 56% of all responding organisations. (Kappelman, 2018) This growth is expected to continue during 2018, since 11.8% of the responding companies has planned cyber-insurance coverage within the next 12 months, at the moment of writing (Kappelman, 2018).

In order to add value for management, this research will explore the possibility of using policies and requirements within cyber insurance as a tool to reduce the amount and impact of cyber attacks. Additionally, decreasing the amount of claims being made. Furthermore, this research will add value for insurance companies by researching how insurance companies can influence the decision of the management of client companies to implement measures of cyber security.

1.1.2. Theoretical relevance

From the scientific point of view, there are several knowledge gaps within cyber-insurance. In an overview of knowledge gaps in the field of cyber insurance, Tøndel, Håkon Meland, Omerovic, Gjære and Solhaug (2015) phrased an interesting gap as a question, *"*Will companies actually implement security improvements in order to obtain cheaper premiums, rather than simply rely on cyber-insurance alone? And how can insurance companies act to reduce moral hazard?*"*. It is therefore unclear how cyber insurance influences the decision to implement cyber security measures and how cyber insurance can be modified in order to reduce the moral hazard. This research aims to contribute to current theoretical knowledge on the decision making process of companies towards cyber security measures as a result of cyber insurance policies. Furthermore, the moral hazard will be taken into account and research will be done into reducing the moral hazard. Besides this, Böhme and Kataria (2006), indicate that a lack of research could be a reason as to why the cyber-insurance market has not matured yet, stating the necessity for more research into cyber insurance.

1.2. Problem Statement

It is unclear how cyber insurance, cyber insurance policies and the level of cyber security of a company influence the management decision to implement measures of cyber security.

1.3. Research Question

In order to handle the problem statement in a proper manner, the necessity arises to divide it into one research question, assisted by four sub questions, as stated below. These questions define more specific areas, which need to be answered in order to be able to solve the problem statement.

Research question:

1. How can cyber insurance policies influence the decision to implement measures of cyber security.

Sub questions:

The first sub question focuses on current issues being faced within cyber security insurance and will aim to answer how they can be solved. Thereafter the second sub question will research the possibilities for cyber security insurance requirements, policy and measures to stimulate companies to

implement new measures. Successive to that, the third question will aim to define, categorize and find a way to measure different types of cyber security measures and their expected results. Subsequently, the fourth and final sub question, will explore the influence of the current level of cyber security of a company in the decision making process to implement extra measures of cyber security. Through these sub questions, the research will provide insights in several ways in order to provide a clear answer on the research question.

1. What are current issues faced within cyber insurance?
2. How can cyber insurance policies stimulate companies to implement new measures of cyber security?
3. What should a cyber security strategy consist of and how can the cyber security level be measured?
4. What is the influence of the current cyber security level in the decision to implement new measures?

1.4. Research Objective

The main objective of this literature review is to get an insight in the influence of cyber insurance on the decision to implement extra measures of cyber security. In order to be able to reach this objective, more insight is required into the factors which can modify insurance policies in order to influence the decision made by management. Furthermore, the cyber insurance market will be studied in order to see if there are challenges within the industry which need to be solved in order for cyber insurance become a mature market.

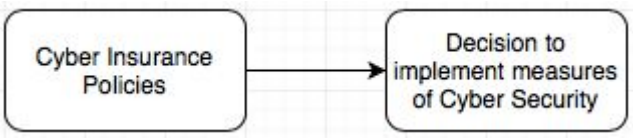


Figure 1, research framework.

1. Cyber Insurance Policies (Independent Variable)
2. Decision to implement measures of Cyber Security (Independent Variable)

1.5. Research Approach

A common approach in forming a bachelor thesis is a literature review. For this bachelor thesis, this approach is put to practice. In this literature review, secondary data from relevant studies and researches is used. The studies and researches used during the literature review will indicate the known concepts and valuable factors in order to reach the demands of the research objective. Based on such literature review the main factors of this research will be: measurements and procedures for cyber security, cyber insurance and the influence it can have on the implementation of cyber security measures by organisations, the influence of requirements, how to measure levels of cyber security,

the influence of a certain level of cyber security on the decision to implement measures of cyber security and contracts in cyber insurance and the possibilities of implementing premiums in cyber insurance.

In order to gather valuable data from studies of high-quality concerning these factors, search engines are used such as: Google Scholar, TiU Library, Sciencedirect and Web of Science. During this search, the aim will be to find recent journals which are applicable on the above stated factors. In order to do so the main searches in the search engines will be conducted on concepts such as insurance, moral hazard, premiums in insurance, cyber insurance, cyber security and cyber attacks. In all cases attention will be paid to reliability and validity of the resources as well as the applicability of the studies and their data.

However, there will always be certain limitations to this type of research which can hardly be reduced. Such limitation are; not being able to find all journals and information regarding the matter due to missing researches when going through search results or because of time limitations.

1.6. Research Structure

The first (and current) chapter clearly indicates a knowledge gap, which this research is aiming to (partially) take away. This chapter also provides the relevance for management. Furthermore, chapter 1 describes the Research Objectives, Problem Statement, Research Questions, Research Methodology and Research Structure.

In Chapter 2, the actual literature research will be conducted. Within this chapter the research aims to clarify what cyber insurance is and what issues it is facing as well as providing a possible solution to these issues. Besides this, the research model will be further elaborated.

Subsequently, chapter 3 will focus on the method which has been used during the research in order to gain the insights which will be presented later on in the research. This chapter will also go into possible issues for companies gathering the data needed to execute the solutions from chapter 2.

Following up on this, Chapter 4 will provide several cases which are to proof the ground for the hypotheses as stated in chapter 2 on the base of previous research.

The fifth and last chapter will summarize the findings from the research, provide discussion points and recommendations for both the implementation of the findings and subjects for future research. Following through, the fifth chapter will offer the conclusion derived from the research.

2. Cyber insurance and the influence on cyber security decisions

2.1. Cyber Insurance

In order to best grasp the concept of cyber insurance and the problems it is facing, first knowledge is required on the differences between cyber risk and conventional risk. Böhme and Schwartz (2010) explain the difference as:

> Two properties distinguish cyber-risk from conventional risk. First, nowadays ICT resources are not isolated machines, but interconnected in a network. Their value largely emerges from this interconnection, therefore the analysis of risk and potential losses must take into account the inter-dependencies between connected nodes. Second, most ICT resources are universal automatons and thus have a dual nature: if operational, they generate value for its operators and therefore become loss sources when they malfunction; moreover, when abused or "taken over" by malicious attackers, benign nodes can become threats to other nodes. (Böhme & Schwartz, 2010, p. 5).

To further understand the market of cyber insurance, it is beneficial to view the model which has been created from the conclusion deriving from the research mentioned above.

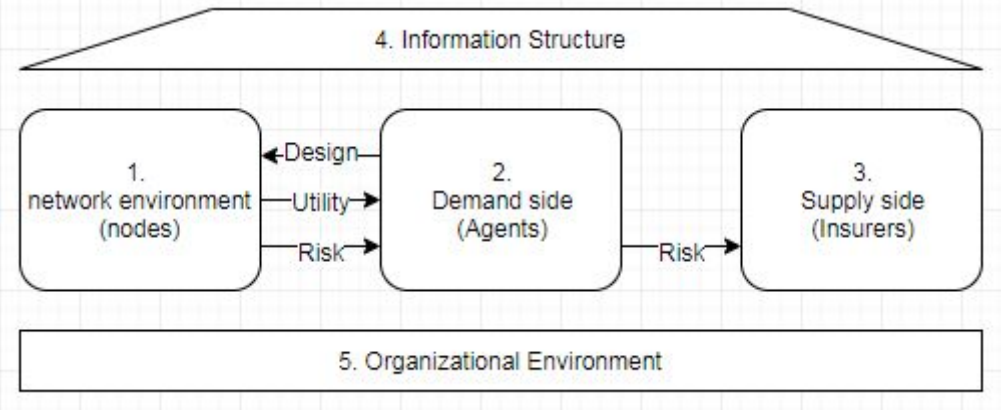


Figure 2. Cyber Insurance market model

1. Network Environment (Nodes), Provides Risk to the agent, provides utility to the agent.
2. Demand Side (Agents), Design a Network Environment, outsource risk to the insurer.
3. Supply Side (Insurers), obtain risk from the agent.
4. Information Structure, influences the environment around the factors.
5. Organizational Risk, influences the environment around the factors.

The model explains the cyber insurance market in a way where the demand side (also stated as the insured or agent) creates a network environment under certain circumstances which lead to a set level of cyber security. This network environment then provides utility to the company, but also results in cyber risk. This risk can then be transferred to the supply side of the insurance (also stated

as the insurer or insurance companies). This model is then also influenced by the information structure and the organizational environment. The information structure influence relies on the effects of information asymmetry between the agent and the insurer. Böhme and Schwartz (2010) explain that "The organizational environment is needed to expand formal models of cyber-insurance markets to a broader system view on cyber-security." (p. 4)

2.1.1 Challenges in (cyber) insurance

However, there are still challenges within the cyber insurance market, which could lead to the failure of a market solution within cyber insurance (Kesan, et al., 2014). In this subchapter, the main challenges being faced within the cyber insurance market will be explained.

Setting a premium: At the moment, setting a premium is difficult for cyber insurance companies due to the lacking of actuarial data and uncertainty within normative standards. This has resulted in high premiums which discourage companies from acquiring cyber insurance coverage. (Toregas & Zahn, 2014) The issue of setting the premium and the viable solutions to this issue will be discussed in 2.2 (Policies, contracts and requirements within Cyber Insurance).

Adverse Selection: The second factor, adverse selection, is best described as the possibility of the client company to know more about the risks which it is, or might be, facing than the insurer. Resulting in the creation of an asymmetry in the information accessible by the insurer and the insured. Which can cause the insurer to miss price the insurance. This will result in only high risk companies insuring themselves, where it is not beneficial for low risk companies to insure. From previous research done in the field of economics (Rothschild, & Stiglitz, 1976), it is known that insurance companies have two possibilities to structure contracts in order to solve this issue, if they are not able to distinguish heterogenous agents. The first being pooling, in this case, a contract is created in which all types of agents are pooled together. The second is separation, in this occasion, insurers create different types of contracts (ranging different contracts from low to high risk). (Rothschild, & Stiglitz, 1976)

Moral Hazard: From the researches of Kappelman, in both 2016 and 2017 it can be found that an increasing amount of companies are making use of cyber insurance packages. However, not all companies will make sure that their firm is well protected when they insure, since the risk and damages are now (partially) at a third party. A study executed by the Dutch Ministry of Justice and Security (2018) found that, in the Netherlands, most firms are not implementing sufficient measures to secure their information, even if they insure themselves. Meaning that, for most of the cases, attacks could have been prevented and damages mitigated if they had made use of basic measures. Böhme and Schwartz (2010) state that "Moral hazard occurs if agents could undertake actions that affect the probability of loss ex post (after the contract is signed and is effective)."

2.1.2 Cyber Insurance Coverage

Besides the cyber insurance industry and the challenges it faces it is also of interest to know what cyber insurance actually covers. Of course this differs per cyber insurance supplier, but in previous research (Kesan et al., 2014) several big cyber insurance coverages were compared. These

companies all make a difference between first party coverage and third party coverage. First party coverage is a type of insurance which covers the insured for damages endured by the insured to the companies property. Third party coverage entails a form of coverage in which the insured cover the company against the liability of damages caused by the company to a third party. (Cannon, 2017). Kesan et al. (2014) explain that under first party coverage fall damages due to “destruction or loss of information assets, internet business interruption, cyber extortion, loss due to denial of service attacks, reimbursement for public relation expenses, and even fraudulent electronic fund transfers”. For most companies, first party cyber insurance coverage is more relevant form, since it protects themselves against damages caused by others to the insured company. Third party cyber insurance coverage is more relevant to companies who supply information technology, as Kesan et al. (2014) state it covers “claims arising from Internet content, Internet security, technology errors and omissions and defense costs”.

Summarizing 2.1, insurance normally results in the agent to neglect the asset or process it has insured. Due to this, adverse selection and moral hazard are major problems for cyber insurance. Hence, a solution needs to be found which can eliminate adverse selection and moral hazard within cyber insurance in order to incentive companies to implement cyber security instead of relying on insurance coverage.

2.2. Policies, Contracts and Requirements within Cyber Insurance

In other insurance industries, such as the car insurance industry, policies such as usage based insurance, the implementation of dynamic pricing, premium differentiation and contract requirements have led to solving issues similar to those which are experienced in the market of cyber insurance. As concluded in the research conducted by Chapados, Bengio, Vincent, Ghosn, Dugas, Takeuchi and Meng (2001), offering different premia which are lower for less risky contracts and higher for more risky contracts can improve the practice of insurance and reduce the cost of the median contract. Deriving from this research, it would be wise to look into factors, which can provide the cyber insurance company, with abilities to overcome moral hazard and adverse selection. As shown by Chapados et al. (2001) policies are used in other markets of insurance to provide an incentive to lower the risk of the insurance being invoked and hence minimizing or even removing the effect of the moral hazard. These policies can be put to use to reward clients who are not reporting claims and punishing those who do, or to punish clients who behave recklessly. In the car insurance industry, for example, the price of a monthly insurance fee gradually goes down when you increase your driver skills and obtain claimless years, the price is differentiated on the basis of your driving style. This creates a premium upon behaviour:

> The Usage Based Insurance (UBI) concept was introduced into the personal motor insurance market over a decade ago. Instead of basing insurance premiums on a vehicle's make and model, the age of driver, their experience and history on the road, UBI assess premiums based upon time of usage, distance driven, driving behavior and places driven to. (EY, 2016)

This creates ground to research if policies in cyber insurance can stimulate companies into implementing cyber security measures?

Unfortunately, there are still problems regarding the implementation of such premiums within the cyber insurance market. Since typically, there are two ways to set a premium within an insurance market. The first of which is based on knowledge derived from actuarial data. Toregas and Zahn (2014) explain that “With actuarial data, insurance companies are looking at past events to determine how likely they are in the future. Sophisticated statistical models exist to determine this likelihood based on a number of factors for mature insurance markets, e.g. car insurance”. Although by now several incidents have happened where companies, institutions or governments have been attacked, it will still be difficult to use this tactic in the cyber insurance industry, since it is simply too new of a market to determine premiums on actuarial data. Therefore the solution needs to be found within the second technique of setting premiums in insurance. This second technique is the use normative standards. Here, Toregas and Zahn (2014) explain that “With normative standards, insurance companies base their calculations on causal relationships between various factors, e.g. someone who never exercises is more likely to suffer from Diabetes”. In order to be able to set premiums through normative standards, factors need to be determined on which the premiums can be differentiated. For cyber insurance the opportunity presents itself to use a similar method as is being used within the car insurance industry. Namely, to differentiate premiums on the cyber security level. (Bolot & Lelarge, 2008) Within recent research (Pal, et al., 2014) it was found that the only way for the cyber insurance industry to improve network security was through discriminating within cyber insurance contracts.

Combining the findings from the researches conducted by Chapados et al. in 2001, EY in 2016, Toregas and Zahn in 2014 and Pal et al. in 2014, precedent is found to add a factor to the cyber insurance market model (Böhme, & Schwartz, 2010). The factor to be added to the model is the influence which cyber insurance policies have on the behaviour of the agent through the implementation of differentiation in contracts.

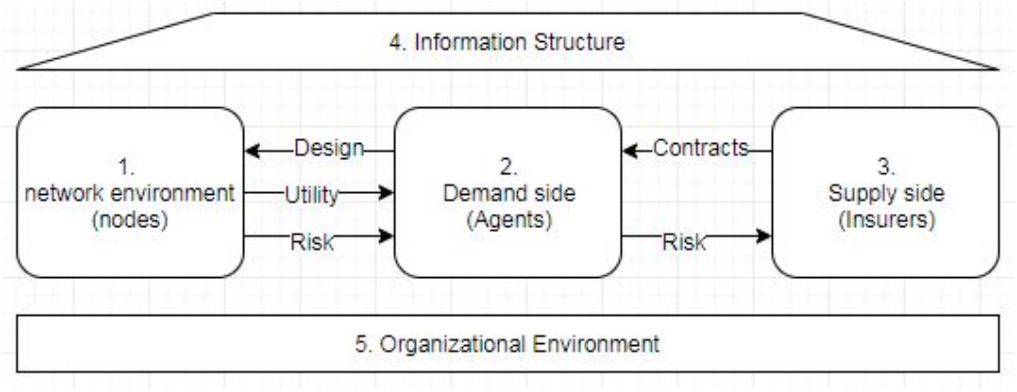


Figure 3. Adjusted cyber insurance market model, **contracts** added.

1. Network Environment (Nodes) Provides Risk to the agent, provides utility to the agent.
2. Demand Side (Agents), Design a Network Environment, outsource risk to the insurer.
3. Supply Side (Insurers), Provide contracts in order to accept the risk from the agent.
4. Information Structure, influences the environment around the factors.
5. Organizational Risk, influences the environment around the factors.

Adding the factor of contracts shows the influence which the insurance company can execute on the agent to stimulate them into improving their network security, which is typically done by increasing or improving measures of cyber security. In order efficiently apply policy to differentiate within contracts, different levels of cyber security need to be able to measured, so that cyber insurance companies can adjust premiums according to the level of cyber security. Within the research of Böhme and Schwartz (2010) several potential designs for contracts have been proposed including the mathematical formulas on which the premium can be set by a cyber insurance company depending on the requirements and preferences of the cyber insurance company. Of the designs proposed in the research of Böhme and Schwartz (2010), the form of premium differentiation provides the best alignment in order for cyber insurance firms to influence the behaviour of management of the agent company into improving the cyber security level. Within this type of design, contracts are tuples offering a certain premium, which is conditional to several aspects amongst which; the security investment of the agent, the risk aversion of the insurance company, the amount of profit the insurance company aims to make and the costs behind the operations. Through this type of contract, agents are stimulated to increase the amount of investment into cyber security and the amount of measures in cyber security.

Summarizing 2.2, policies and requirements within contracts, such as differentiating on premiums between levels of cyber security, reduces the effect of adverse selection and moral hazard in the cyber insurance market. Through these forms of cyber insurance policies, the decision of management to implement measures of cyber security is positively influenced.

2.3. Cyber Security Level

In order for cyber insurance companies to be able to differentiate on different levels of security amongst agents, it is necessary to know where different levels of cyber security come from and how they can be measured. Subsequently to this, insurance companies can then determine which premium they want to apply to certain levels of cyber security. In order to correctly define and categorize the measures, which can be used to increase the level of cyber security of a firm, several vulnerabilities are assessed and different measures, which can be used to eliminate or decrease threats are explored. These measures are divided into three different categories; prevention, detection and response.

2.3.1. Intrusion Prevention Systems

All systems have vulnerabilities due to interaction with humans. Humans are subject to mistakes and errors, which can lead to vulnerabilities at a firm. (Ponemon Institute, 2012). Karjalainen and Siponen (2010) describe this issue such that “Employees’ non-compliance with IS security procedures is a key concern for organizations. To tackle this problem, there exist several training approaches aimed at changing employees’ behavior”. A clear tatic to minimize the faults and vulnerabilities caused by human interaction with a system is to create more awareness amongst employees and train users. Abawajy (2012) states that “Information security awareness can be

defined as the level of comprehension that users have about the importance of information security best practices." Abawajy (2012) also found that "there is ample evidence that security awareness training is the most cost-effective form of security control. Since human error and negligence is the number one cause for data breaches (Ponemon Institute, 2012), this is one of the most important vulnerabilities to address.

Besides covering the aspect of the human error, there is also the technological aspect of cyber attack prevention. According to recent research (Sreevathsa, Daina, Hemalatha & Manjula, 2016), a firewall is any kind of software or hardware, which prevents unusual activity. It does this by maintaining traffic over the internet, both incoming and outgoing interaction. Therefore, a firewall functions as a filter to restrict the entering of certain packets, which are found to be suspicious. During recent research (Da Costa Júnior, Eduardo da Silva, Pinheiro, & Sampaio, 2018) the possibility for a self-adaptive distributed firewall system to reduce the exposure windows of vulnerabilities in the systems was studied. Compared to self-adaptive firewalls, normal distributed firewalls have a weakness:

> Distributed firewalls emerged with the proposal of protecting individual hosts against attacks originating from inside the network. In these systems, firewall rules are centrally created, then distributed and enforced on all servers that compose the firewall, restricting which services will be available. However, this approach lacks protection against software vulnerabilities that can make network services vulnerable to attacks, since firewalls usually do not scan application protocols. (Da Costa Júnior, et al., 2018)

Through the experiments conducted in the research of Da Costa Júnior et al. (2018), the feasibility of a self-adaptive distributed firewall was proved. Which enables a firewall to be dynamic and modify itself on protected servers. Through this work it can be stated that the implementation of self-adaptive distributed firewalls is a valuable improvement on firewall systems.

2.3.2. Intrusion detection systems

In the research conducted by Ye, Zhang and Borror (2014) into "the robustness of the Markov-chain model for cyber-attack detection", intrusion detection is explained to be "used to identify cyber-attacks while they are acting on a computer and network system to compromise the security (e.g., availability, integrity, and confidentiality) of the system". In order to detect abnormalities in activities in the system whilst they're occurring, several intrusion-detection methods can be used. During this research we will highlight four of the most common methods, namely; Intrusion Detection Systems (IDS), Misbehavior detection, signature based approach and anomaly detection.

Intrusion Detection System (IDS) The first method is the usage of an IDS, a method which is highly relied on by security analysts. The systems is used to detect intrusions and misuse within networks by matching current network activities with patterns which are known to align with attacks. In the event that the IDS signals an abnormality in the activities or an attack it will produce an alert. However, in IDS, decreasing the amount of missed attacks inflates the amount of false alerts reported by the system (Green & Swets, 1966). Unfortunately due to the continuing complexity of cyber attacks

being executed by criminals, the number of alert reported by an IDS can be too overwhelming to a human analyst. In addition to this, about 99% of these alerts are based on false alerts. (Goodall, Lutters & Komlodi, 2004). This causes an IDS to be an effective measure to detect attacks but also causes it to result in high costs due to the workforces needed to assess all the incoming alerts.

Host intrusion detection. As derived from a survey conducted by Stiawan, Shakhatreh, Idris, Bakar and Abdullah (2012), host intrusion detection methods are best explained as a specification of a technique during which the systems resides on and monitors only one individual host machine. Host intrusion detection is divided into two categories, namely; Misbehavior/misuse detection and the signature approach method. The general idea of misbehavior/misuse detection according to Raiyn (2014), is to match sets of events with predefined sets of events which are known to be linked to attack techniques. This also directly shows the vulnerability of this way of detecting attacks, since it can only detect those attacks which are already known, not the newly developed forms of cyber attacks. The signature based approach is more thorough in detecting intrusions when compared to the misbehavior detection technique (Raiyn, 2014).

Anomaly detection. Anomaly detectors identify abnormal behavior within a host or network (Kim, Park & Lee, 2013). Gomez and Dasgupta (2001) explain that, “they function on the assumption that attacks are different from legitimate activity and can therefore be detected by systems that identify these differences”.

2.3.3. intrusion Response Policies and Procedure

Besides cyber security measures categorized as prevention and detection measures, attention has to be paid to measures which can mitigate damages in the unfortunate event that an cyber attack or data breach occurs. These measures are categorized as intrusion response policies and procedures. Amongst these procedures fall the implementation of an action plan, guiding what to do in the case of such an event. These steps should then be followed in order to mitigate damages due to loss of image/reputation, be compliant with laws and make sure that the attacker is not able to cause more damage. Leighton (2013), in his book the “Computer Incident Response and Forensics Team Management : Conducting a Successful Incident Response”, provides a research based advise on how to respond when an incident occurs. Concluding from his research the following is described as a best practice method to approach an incident.

Assembling a Security Incident Response Team (SIRT), the SIRT has the purpose to make sure that all necessary resources are made available and to structurally deal with incident. In order to reach this purpose the research of Leighton (2013) states that “the security incident response process is centered on the preparation, detection and analysis, containment, investigation, eradication, recovery and post incident activity surrounding such an incident”. Within his research, Leighton (2013) also states seven steps, which are to be followed by the SIRT in order to efficiently deal with the incident.

Additional to these seven steps, several other steps need to be taken in order to be compliant with the GDPR and to limit the increase of damage due to an incident. The inflicted company has to

act according to the detailed steps as described in Article 33 of the General Data Protection Regulation by the Council of the European Union (2015).

Besides the different types of security measures and the influence they have on the cyber security level it is also interesting to know the effect, which the cyber security level has on the decision process to implement cyber security measures. Since that adverse selection is still a problem within cyber insurance (Kesan et al. 2014), momentarily companies with a low level cyber security level tend to acquire cyber insurance, where companies with a high cyber security level tend not to acquire cyber insurance. When differentiated premiums are implemented within cyber insurance, as proposed in chapter 2.2, an incentive arises which changes this effect. Since, it becomes more interesting for companies with a high cyber security level to acquire cyber insurance. Subsequently, it becomes interesting for companies with a low cyber security level (in possession of cyber insurance) to increase the cyber security level. Through increasing the cyber security level companies are granted with a lower monthly premium. For companies with a low cyber security level this effect is higher since they stand more to gain on the cyber security level and hence have more options to decrease the monthly premium and can decrease this premium with a larger amount than companies with a high security level can.

Summarizing 2.3, a lower level of cyber security increases the influence which cyber insurance policies have on the decision of management to implement measures of cyber security and vice versa. Upon this, a higher level of cyber security, directly negatively influences the decision to implement cyber security measures and vice versa. Furthermore, cyber security measures have been categorized within three types; intrusion prevention, intrusion detection and intrusion response measures. On the basis of the measures cyber insurance companies can differentiate on the cyber security level of an agent company, find areas for improvement and adjust the premium accordingly.

2.4. Decision to implement measures of cyber security

In order to be able to fully research the influence of cyber insurance policies on the decision to implement cyber security measures it is necessary to study the decision process by management of how to allocate cyber security investments. According to Deloitte and NASCIO (2014), the main challenge in allocating cyber security investments for chief information security officers (CISO) is that they receive insufficient funding (especially amongst small and medium enterprises), in order to properly secure the company which the CISO works for. In research conducted on the subject of decisions on cyber security investments (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016) several approaches are studied. Within this research, the challenge of having insufficient funding for cyber security is acknowledged and taken into account when proposing approaches. During the research of Fielder et al. 2016, they consider the cost of a certain cyber security measure, the indirect cost and its influence on the networks defence to be the main determines to compare measure on. Within these boundaries, several approaches are used to see which cyber security measures are most valuable to the company. The approaches which are studied by Fielder et al. (2016) are that of game theory, combinatorial optimisation and a hybrid method between the two. However, in every

case within the experiment conducted in the research of Fielder et al. 2016, the management decisions are made within budgetary boundaries, which the CISO's believe to be insufficient. As stated in chapter 2.1, cyber insurance can be used to cover damages which can come forth from insufficiently defending of a company. Therefore, for small and medium enterprises lacking funding, cyber insurance provides a solution. Upon covering for potential damages, cyber insurance (through policies) can provide the CISO with an incentive to implement cyber security measures whilst staying in the budget. This, since the increased cyber security level can lead to a lower monthly premium for cyber insurances which apply differentiated premiums as explained in chapter 2.2 and 2.3. In the conclusion of the research of Fielder et al. 2016, cyber insurances are also proposed as an incentive to influence the decision to implement cyber security measures.

2.5. Hypotheses and Interdependence

These hypotheses explain the influence which each of the variables have within the research model as stated below.

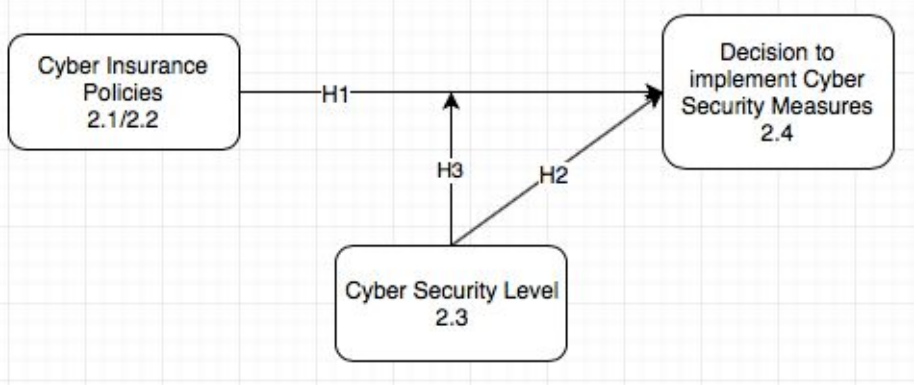


Figure 4. Expanded research model

A = Cyber Insurance Policies (Independent Variable)

B = Level of Cyber Security (Moderator)

C = Decision to implement measures of cyber security (Dependent Variable)

H1). Cyber Insurance policies have a positive influence on the decision of management to implement measures of cyber security.

H2). The level of cyber security also has a negative influence on the decision to implement measures of cyber security. Meaning, the higher the current level of cyber security of an agent company is, the less the influence of cyber insurance policies on the decision to implement measures of cyber security is and vice versa.

H3). The level of cyber security also has a negative moderating effect on the influence which cyber insurance policies have on the decision to implement cyber security measures. Meaning, how higher the level of cyber security, less influence is seen from cyber insurance policies on the decision to implement measures of cyber security.

The positive influence of A on C

A (cyber insurance policies) has a positive effect on C (decision to implement measures of cyber security). In chapters 2.1 and 2.2 cyber insurance and the possibilities to implement certain policies in cyber insurance have been researched. Collecting all the knowledge it provides ground that cyber insurance policies, such as premium differentiation have a positive influence on the insured to not only acquire insurance but to also increase the cyber security level by investing in measures of cyber security.

The negative influence of B on C

B (cyber security level) has a negative influence on C (decision to implement cyber security measures). In chapter 2.3 it is argued that an increased level of cyber security results in a negative influence on the decision to implement cyber security measures, since the necessity to acquire a higher level of cyber security becomes less important for a higher current cyber security level.

The effect of B on the influence of A on C

B (cyber security level) has a negative effect on the influence which A (cyber insurance policies) has on C (decision to implement cyber security measures. In chapter 2.3 an argument similar to that which argues the negative influence of B on C is presented. Since, if the current cyber security level of company A is lower compared to company B, company A will stand more to gain in a differentiated premium structure than company B. Causing the cyber insurance policies to have a higher influence on companies with a lower cyber security level.

3. Methodology

In order to be able to assess the value of this research in a correct manner, it is of importance to view the method through which data is collected and which restraints this method might face or the influence it could have on the validity and reliability of the conducted research.

3.1. Data collection method

During this research several ways have been used in order to gather relevant information to be obtained in the research. The largest amount of content is taken from esteemed journals which have been found online by searching several online libraries and search engines. The search engines which were used during the research are the following; Google Scholar, TiU Library, Sciencedirect and Web of Science. Within these search engines the following search terms were used; Cyber Security Measures, Cyber Insurance, premiums in Insurance, Moral Hazard, Adverse Selection, intrusion detection and prevention methods, security incident response and Digital Resilience. Besides this, content has been gathered through publications of institutions within the Dutch Government.

3.2. Limitations to data collection method

In order to ensure that research is valued correctly, limitations of the data collection are addressed. The following limitations are relevant to this literature review; missing information, due to restrictions in time and access, information with relevance to the research can be neglected or missed out on. The restriction of access is due to the fact that some papers are only fully accessible if you study at certain universities or if you have a paid subscription for certain journals or scientific magazines. Through a student account at Tilburg University some of these sources can still be accessed, unfortunately others can not. Furthermore, a limitation in the data collection is present due to the scarcity of data. The cyber insurance industry is a relatively new developed industry, due to which there are still knowledge gaps which impede the collection of data.

3.3. Data obtainment

Besides the data collection method executed during this literature review, some notes are also to be given with regards to the data collection of cyber insurance companies. In order for cyber insurance companies to collect the data needed for the actuarial method of premium setting, some constraints need to be kept in mind. In order to best regard the privacy and safety of agent companies, the insurance companies need to comply to the General Data Protection Regulation by the Council of the European Union (2015) and should be safely stored and anonymized.

4. Results and Case studies

4.1. Results

4.1.1 Managerial Implications

The managerial implications of this literature review are mostly relevant to management of cyber insurance companies and companies wanting to implement cyber security. For cyber insurance companies this research has provided interesting knowledge resulting in the ground of cyber insurance policies to influence agent company behaviour. Through the implementation of premium differentiation, cyber insurance companies can better align the risk of an agent with their premium. Leading to the market to become more interesting for low risk firms and hence an increase in demand. For companies looking to acquire cyber security, the research provides an overview of best practices for each of the three categories of cyber security measures.

4.1.2. Contribution to research

Through the gathering of information on the cyber insurance industry and the possibilities for policies within cyber insurance contracts, information was found which suggests that, if premium differentiation is correctly implemented, this will lead to companies actually implementing cyber security measures instead of relying on cyber insurance. With this, an uncertainty in the current overview of knowledge surrounding cyber insurance is cleared. This leads to the possibility for further research to be conducted on the bases of this result without assumptions clouding the reliability of the research.

4.2. Case studies

4.2.1. Case Study: Contracts and Requirements as a solution to Adverse Selection and Moral Hazard within the Cyber Insurance Industry

According to Kesan et al. (2014), the main problems for the cyber insurance market are adverse selection and moral hazard. If these problems were to be solved, this would have several benefits. Kesan et al. (2014) explain that “Cyber insurance would result in higher security investment, increasing the level of safety for information technology infrastructure”. Upon this, Kesan et al. (2014) express that “cyber insurance can facilitate standards for best practices as cyber insurers seek benchmark security levels for risk management decision-making”. The last benefit being highlighted is that of a higher overall societal welfare. The findings of the case study conducted by Kesan et al. (2014) are aligned with those of this literature review. In the case study, Kesan et al. (2014) also provides a viable solution to the issues of adverse selection and the moral hazard within the cyber insurance industry. It is proposed that cyber insurance can complement self-protection, but only if premiums are tied do different levels of self-protection by client companies (Figure 5).

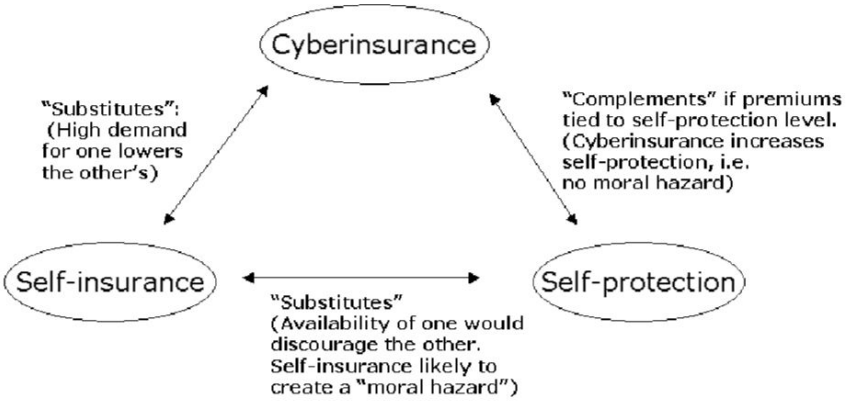


Figure 5; Cyber insurance, self-insurance and self-protection

4.2.2. Case Study: the decision of cyber security investment

Within the research conducted by Fielder et al. 2016, a case study is included to test which of the researched methods (full game theory, pure knapsack or a hybrid) is best to use when approaching the decision of the cyber security investment. Through their case study Fielder et al. (2016) found that generally "the Full Game representation will provide a better defence to the weakest target for low budget levels". Additionally Fielder et al. found that "the Hybrid is occasionally able to offer a better solution than the Pure Knapsack, because the mixed strategies allow for certain control combinations to be used at a lower budget". However, this case study also indicates that, due to lacking budget for cyber security, vulnerabilities are often left open. Cyber insurance provides a solution in order to cover potential losses for companies with insufficient budget and incentives the management to secure additional budget for cyber security if premium differentiation is adopted in the cyber insurance package.

5. Conclusion and recommendations

5.1. Conclusive remarks

Combining the knowledge from previous research, the literature review has found precedent in order to answers the questions stated in chapter 1.3 of the literature research. By implementing cyber insurance policy, such as premium differentiation, the decision to implement cyber security measures is positively influenced. Cyber insurance companies can differentiate on the cyber security level and investments in order to divide lower and higher risk agents and price them accordingly. Subsequently, the cyber security level of a company influences both the effect of the cyber insurance policies, as the decision to implement cyber security measures itself, negatively. Meaning that, an increase in the cyber security level results in a decrease in the effect of cyber insurance policies as well as a decrease in the decision to implement cyber security measures. It is also discovered that the cyber insurance market is facing issues of adverse selection and moral hazard, which can both be solved through cyber insurance policy implementation. Furthermore, it is concluded that if premium differentiation is implemented, cyber insurance can improve network security by stimulating companies to implement cyber security measures.

5.2. Recommendations

5.3.1. Managerial recommendations

Through the conclusion of this literature review, it is recommended to cyber insurance companies to implement policies of premium differentiation. This will result in an incentive to increase the cyber security level by implementing or improving cyber security measures. Furthermore, cyber insurance companies are recommended to include clauses in the contracts to enforce regular observing of the cyber security level in order for positive and negative changes to be detected in the cyber security level. Cyber insurance companies are also advised to calculate differentiated premiums on the base of normative standards and differentiate on cyber security levels and investments. Cyber insurance companies are also recommended to establish a security incident response team (SIRT), which is to be deployed in the case of an incident at a company without the means to establish a SIRT themselves.

5.3.2. Future research opportunities

Future research should focus on actuarial data collection from cyber attacks in order to improve differentiated premium calculations. Through this research on actuarial data, more knowledge will be gathered on the precise relation between the cyber security level and the chance of a cyber attack and the relative inflicted damage. Future research should also be conducted on how government institutions can influence the cyber insurance industry and into the impact which this can have on the cyber insurance market.

References

1) *Karjalainen, M., & Siponen, M. (2010, 31 maart). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. Retrieved, 24 October 2018, from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1584*

2) *Abawajy, J. (2012, February 10). User preference of cyber security awareness delivery methods [Vol. 33, No. 3, 237–248]. Geraadpleegd op 9 november 2018, van Journal Behaviour and Information Technology, https://www.tandfonline.com/doi/abs/10.1080/0144929x.2012.708787*

3) *Böhme, R., & Kataria, G. (2006, June). Models and Measures for Correlation in Cyber-Insurance. Retrieved, December 1, 2018, from http://sec2013.crysys.hu/~mfelegyhazi/courses/EconSec/readings/09_BohmeK2005insurance_correlation.pdf*

4) *Böhme, R., & Schwartz, G. (2010, May 21). Modeling Cyber-Insurance: Towards a Unifying Framework [Conference Paper]. Retrieved, November 8, 2018, from http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf*

5) *Bolot, J. C., & Lelarge, M. (2008). A New Perspective on Internet Security using Insurance. In IEEE INFOCOM 2008 - The 27th Conference on Computer Communications. IEEE. https://doi.org/10.1109/infocom.2008.259*

6) *Cannon, P. (2017, September 6). What is the Difference Between First-Party Insurance vs Third-Party Insurance? Retrieved, December 7, 2018, from https://www.simmonsandfletcher.com/blog/difference-first-party-insurance-vs-third-party-insurance/*

7) *Chapados, N., Bengio, Y., Vincent, P., Ghosn, J., Dugas, C., Takeuchi, I., & Meng, L. (2001, December 8). Estimating car insurance premia: a Case Study in High-Dimensional Data Inference. Retrieved, November 18, 2018, from http://papers.nips.cc/paper/2062-estimating-car-insurance-premia-a-case-study-in-high-dimensional-data-inference.pdf*

8) *Cisco. (2018). What Are the Most Common Cyberattacks? Retrieved, November 16, 2018, from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html*

9) *Council of the European Union. (2015, 18 december). General Data Protection Regulation. Retrieved, November 14, 2018, from https://www.rijksoverheid.nl/documenten/rapporten/2016/01/07/tk-bijlage-1-council-of-the-european-union*

10) *Da Costa Júnior, E., Eduardo da Silva, C., Pinheiro, M., & Sampaio, S. (2018, June 4). A new approach to deploy a self-adaptive distributed firewall. Retrieved, December 2, 2018, from https://jisajournal.springeropen.com/track/pdf/10.1186/s13174-018-0083-6*

11) *Deloitte & NASCIO. (2014). Deloitte NASCIO Cybersecurity Study. Retrieved, December 8, 2018, from http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf*

12) *EY. (2016). Introducing " Pay How You Drive " (PHYD) Insurance. Retrieved, November 10, 2018, from https://www.ey.com/Publication/vwLUAssets/ey-introducing-pay-how-you-drive-insurance/$FILE/ey-introducing-pay-how-you-drive-insurance.pdf*

13) *Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016, March 19). Decision support approaches for cyber security investment. Retrieved, December 8, 2018, from https://www.sciencedirect.com/science/article/pii/S0167923616300239*

14) *Gomez, J. & Dasgupta, D. (2001, June). "Evolving Fuzzy Classifiers for Intrusion Detection", Proceeding of the IEEE Workshop on Information Assurance, United States Military Academy*

15) *Goodall, J.R., Lutters, W.G., Komlodi, A. (2004), I know my network: Collaboration and expertise in intrusion detection. J. Herbsleb, G. Olson (Eds.), Proceedings of the 2004 ACM conference on computer supported cooperative work, ACM, New York, NY (2004), pp. 342-345. Retrieved, November 12, 2018.*

16) *Green, D.M. , Swets, J.A., 1966 Signal detection theory and psychophysics. Retrieved, November 12, 2018*

17) *Kappelman, L., Nguyen, Q., McLean, E., Maurer, C., Johnson, V., Snyder, M., & Torres, R. (2017, March). The 2016 SIM IT Issues and Trends Study. Retrieved, September 19, 2018, from http://www.misqe.org/ojs2/index.php/misqe/article/viewFile/749/452*

18) *Kappelman, L., Nguyen, Q., McLean, E., Maurer, C., Johnson, V., David, A., & Torres, R. (2018, March). The 2017 SIM IT Issues and Trends Study. Retrieved, September 19, 2018, from https://misqe.org/ojs2/index.php/misqe/article/viewFile/818/484*

19) *Kesan, J., Marjuca, R., & Yursic, W. (2014, June 5). Cyber insurance as a market-based solution to the problem of cyber security - a case study. Retrieved, December 4, 2018, from https://www.researchgate.net/profile/Jay_Kesan/publication/228669949_Cyberinsurance_as_a_market-based_solution_to_the_problem_of_cybersecurity_a_case_study/links/00b495248e89c569f9000000.pdf*

20) *Kim, A. C. , Park W. H., & Lee, D. H. (2013). "A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals", International Journal of Network Security, vol. 7, no. 1, pp. 181-188*

21) *Mather, D. (2018, January 30). Dutch Banks Targeted in DDoS Cyber Attacks. Retrieved, November 8 2018, from https://securityzap.com/dutch-banks-ddos/*

22) *Ministry of Justice and Security. (2018, August 7). Cyber Security Assessment Netherlands 2018. Retrieved, September 12, 2018, from https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html*

23) *Pal, R., Golubchik, L., Psounis, K., & Hui, P. (2014). Will cyber-insurance improve network security? A market analysis. In IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. IEEE. https://doi.org/10.1109/infocom.2014.6847944*

24) *Ponemon Institute. (2012) The human factor in data protection. Retrieved, November 11, 2018 from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey–2012.pdf*

25) *Raiyn, J. (2014). A survey of Cyber Attack Detection Strategies. Retrieved, November 12, 2018, from https://pdfs.semanticscholar.org/942a/4ce3f6ddadc5bbdd55497861dc8c85703cdd.pdf*

26) *Rothschild, M., & E. Stiglitz, J. (1976, November). Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. [The Quarterly Journal of Economics, 90(4):630–49]. Retrieved, November 9, 2018, from https://www.jstor.org/stable/1885326?origin=JSTOR-pdf&seq=21#metadata_info_tab_contents*

27) *Solms, R., & Niekerk, J. (2012, November 26). From information security to cyber security. Retrieved, December 5, 2018, from https://www.sciencedirect.com/science/article/pii/S0167404813000801*

28) *Sreevathsa C.V, Daina K.K, Hemalatha K.L, & Manjula K. (2016). Increasing the performance of the firewall by providing customized policies. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). IEEE. https://doi.org/10.1109/icatcct.2016.7912063*

29) *Stiawan, D. , Shakhatreh, A. I., Idris, M. Y. , Bakar K. A. & Abdullah, A. H. (2012). "Intrusion Prevention System: A Survey", Journal of Theoretical and Applied Information Technology, vol. 40, no. 1, pp. 44-54*

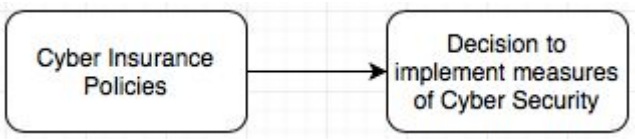
30) *Tøndel, I., Håkon Meland, P., Omerovic, A., Gjære, E., & Solhaug, B. (2015, November 11). Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research. Retrieved, September 18, 2018, from https://brage.bibsys.no/xmlui/bitstream/handle/11250/2379189/SINTEF%2bA27298.pdf?sequence=3&isAllowed=y*

31) *Toregas, C., & Zahn, N. (2014, January 7). Insurance for Cyber Attacks: The Issue of Setting Premiums in Context. Retrieved, September 13, 2018, from https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/cyberinsurance_paper_pdf_0.pdf*

32) Ye, N., Zhang, Y., & Borror, C. M. (2004). Robustness of the Markov-Chain Model for Cyber-Attack Detection. IEEE Transactions on Reliability, 53(1), 116–123. https://doi.org/10.1109/tr.2004.823851

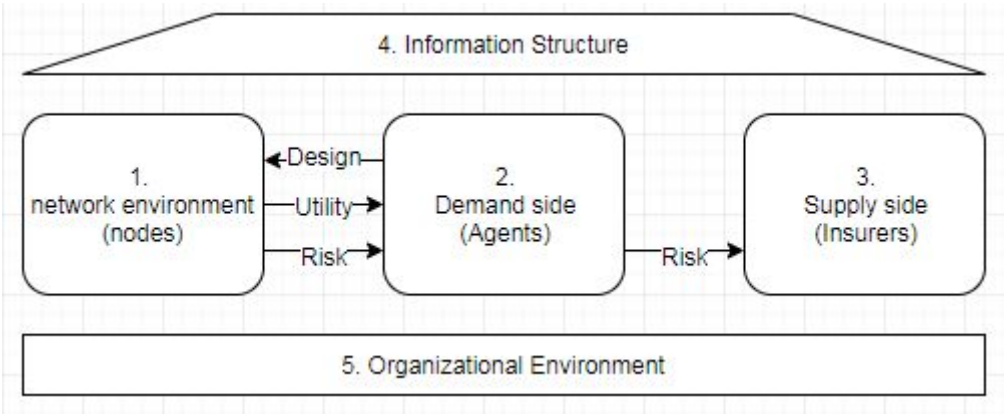
Appendixes

Figure 1. Research Model



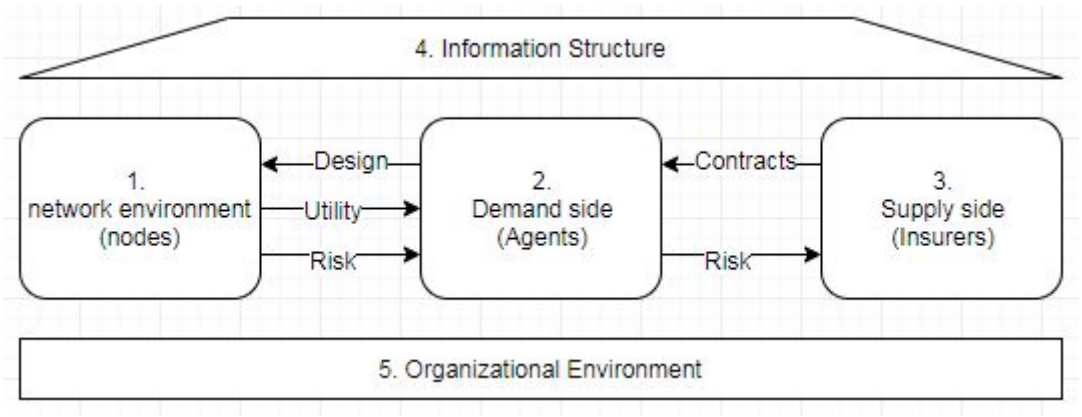
1. Cyber Insurance Policies (Independent Variable)
2. Decision to implement measures of Cyber Security (Independent Variable)

Figure 2. Cyber Insurance Market Model (Adapted from Böhme and Schwartz 2010)



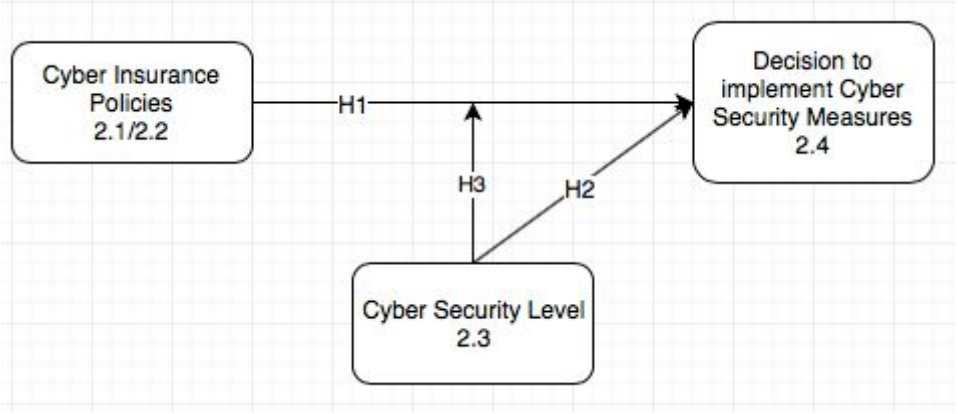
1. Network Environment (Nodes), Provides Risk to the agent, provides utility to the agent.
2. Demand Side (Agents), Design a Network Environment, outsource risk to the insurer.
3. Supply Side (Insurers), obtain risk from the agent.
4. Information Structure, influences the environment around the factors.
5. Organizational Risk, influences the environment around the factors.

Figure 3. Adjusted cyber insurance market model (Contracts added)



1. Network Environment (Nodes), Provides Risk to the agent, provides utility to the agent.
2. Demand Side (Agents), Design a Network Environment, outsource risk to the insurer.
3. Supply Side (Insurers), Provide contracts in order accept the risk from the agent.
4. Information Structure, influences the environment around the factors.
5. Organizational Risk, influences the environment around the factors.

Figure 4: Expanded research model



2.1 / 2.2	Cyber Insurance Policies (Independent Variable)
2.3	Level of Cyber Security (Moderator)
2.4	Decision to implement measures of cyber security (Dependent Variable)

Figure 5: Strategies to deal with cyber-risk (adapted from Kesan, Majuca, Yurcik 2004:13)