CYBECO

Supporting Cyberinsurance from a Behavioural Choice Perspective

D7.1: CYBECO Policy Recommendations

Due date: M24

Abstract:
This CYBECO deliverable describes the project's study on policy recommendations regarding cyberinsurance. It reports the results of research to identify possible gaps in key directives and standards, evaluate them in the light of CYBECO findings, and suggest ways of overcoming them with recommendations for policy design and practice. The starting point for this work was an investigation of the cyberinsurance ecosystem and how it is organized, identifying the main and secondary stakeholders, their goals and relations between them. In the next step, we investigated existing and proposed policy measures for cyberinsurance, their mapping onto the goals of the main actors, and their coverage in regulation, in order to identify the possible gaps. To inform future policy, we studied how cyber insurance decision-making is done in the wild through two empirical studies with stakeholders in the EU. We also developed an agent-based model to investigate the effects of various policy interventions on the overall level of risk in the ecosystem. This all-around approach helped us to identify several policy recommendations aiming to improve the cyberinsurance ecosystem.

Dissemination Level		
PU	Public	x
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document Status

Document Title	CYBECO Policy Recommendations
Version	1.0
Work Package	7
Deliverable #	7.1
Prepared by	Katsiaryna Labunets & Wolter Pieters (TUDELFT)
Contributors	Pieter van Gelder & Michel van Eeten (TUDELFT), Dawn Branley-Bell, Pam Briggs & Lynne Coventry (UNN), Josè Vila & Yolanda Gómez (DEV-STAT)
Checked by	UNN
Approved by	TREK
Date	30-04-2019
Confidentiality	PU

Document Change Log

Each change or set of changes made to this document will result in an increment to the version number of the document. This change log records the process and identifies for each version number of the document the modification(s) which caused the version number to be incremented.

Change Log	Version	Date
Changes description	0.1	Aug 27, 2018
Internal draft	0.2	Apr 15, 2019
Updated abstract, introduction section, and chapter 5	0.3	Apr 15, 2019
Addressed comments from UNN and TUDELFT	0.4	Apr 24, 2019
Updated final set of recommendations and addressed comments from DEVSTAT	0.5	Apr 26, 2019
Final version	1.0	Apr 30, 2019

Table of Contents

1 Introduction **8**
1.1 Objectives and Scope . . . 8
1.2 Document Structure . . . 8

2 Cyberinsurance ecosystem **9**
2.1 Cyberinsurance . . . 9
2.2 Cyberinsurance actors and relationships . . . 11
2.2.1 Main actors . . . 11
2.2.2 Secondary actors . . . 13
2.3 Goals of the main actors . . . 15
2.3.1 Insurance provider . . . 16
2.3.2 Intermediary . . . 16
2.3.3 SMEs . . . 16
2.3.4 Policymakers/Government . . . 16
2.4 Conclusion . . . 16

3 A framework of policy measures and cyberinsurance **17**
3.1 Framework of Policy Measures for Cyber Insurance . . . 17
3.1.1 Wider adoption . . . 17
3.1.2 Defining coverage . . . 18
3.1.3 Data collection . . . 18
3.1.4 Information sharing . . . 18
3.1.5 Best practices . . . 19
3.1.6 Catastrophic loss . . . 19
3.2 Mapping of policy measures on ecosystem actor goals . . . 20
3.3 Ethical considerations . . . 22
3.4 Conclusions . . . 24

4 Cyberinsurance in current cyber security directives and standards **25**
4.1 Wider adoption: legislation assigning financial costs to cyber events . . . 25
4.2 Best practices: requiring certain level of cyber security from organizations . . . 26
4.3 International standard for cyberinsurance . . . 28
4.4 Conclusions . . . 28

5 Empirical investigation of policy usability **29**
5.1 Background . . . 29
5.2 Method . . . 31
5.3 Results – Phase 1: Risk registers, insurance policies and business security policies 32
5.4 Results – Phase 2: Stakeholders Interviews . . . 33
5.4.1 Complexity of the company-level decision-making process . . . 33
5.4.2 Internal conflict around cyberinsurance adoption . . . 34
5.4.3 Compliance Legislation as a driver for cyberinsurance adoption . . . 37
5.5 Conclusion . . . 38

6 Cyberinsurance adoption among Dutch SMEs: a qualitative study **40**
6.1 Protection Motivation Theory for cyberinsurance . . . 41
6.2 Research method and study execution . . . 42
6.2.1 Data collection . . . 42
6.2.2 Data analysis . . . 42
6.3 Results . . . 44
6.3.1 Sources of information . . . 44
6.3.2 Threat appraisal . . . 45
6.3.3 Coping appraisal . . . 46
6.3.4 Drivers and impediments . . . 47
6.3.5 A Model of Cyber Insurance Adoption among SMEs . . . 48
6.4 Conclusions and discussion . . . 50
6.4.1 Component: Source of Information . . . 50
6.4.2 Component: Threat Appraisal . . . 52
6.4.3 Component: Coping Appraisal . . . 52

7 Simulating policy effects with agent-based modelling **53**
7.1 Model design . . . 53
7.2 Results . . . 55
7.3 Conclusions and discussion . . . 55

8 Discussion on policy recommendations **58**
8.1 Summary of findings . . . 58
8.2 Results from Lorentz seminar . . . 59
8.3 Final recommendations . . . 60

List of Figures

2.1 Cyberinsurance contract agreement process 10
2.2 Cyberinsurance ecosystem 12

5.1 Focusing upon the company within the cyberinsurance ecosystem 29
5.2 Burke and Litwin Organisational Performance and Change Model 30

6.1 Cyberinsurance adoption model (Martinez Bustamante 2018) 49
6.2 SEM model of cyberinsurance adoption 51

7.1 The simplified ecosystem for the agent-based model (Sewnandan 2018). 53
7.2 The flow diagram of the agent-based model (Sewnandan 2018). 54
7.3 The interface of the agent-based model in NetLogo (Sewnandan 2018). 54
7.4 Effects of policy options on global security strength (Sewnandan 2018). 56
7.5 Effects of policy options on global value loss (Sewnandan 2018). 56
7.6 The number of insured organisations per policy option over time (Sewnandan 2018). 57

List of Tables

3.1 Mapping of policy measure themes on ecosystem actor goals 21

5.1 Interviewee experience/background 31

6.1 Questionnaire for SMEs per scenario (Martinez Bustamante 2018) 43
6.2 Demographics of interviewed SMEs (Martinez Bustamante 2018) 44
6.3 Number of codes per PMT elements, drivers and impediments 44
6.4 Co-occurrence of codes and PMT elements related to the source of information component 45
6.5 Co-occurrence of codes and PMT elements related to the threat appraisal component 45
6.6 Co-occurrence of codes and PMT elements related to the coping appraisal component 47
6.7 Co-occurrence of drivers, impediments and codes 48

1 Introduction

1.1 Objectives and Scope

The objective of this deliverable is to identify possible gaps in key directives and regulations, evaluate them in the light of CYBECO findings and suggest ways of overcoming them, with recommendations for policy design and practice. With this aim, we started with an investigation on how the cyberinsurance ecosystem works, what actors are involved in the cyberinsurance process and what goals they have. Next, we analyzed how known policy measures are mapped onto the goals of the main actors and identified the policy gaps. We also checked existing cyber security regulations on how they related to the cyberinsurance ecosystem and identified policy measures. We conducted two empirical studies with stakeholders in the EU to investigate how the decision-making process works around cyberinsurance matters. We applied a modeling exercise based on the agent-based model of cyberinsurance ecosystem, to explore the effects of different types of policy interventions on the overall level of risk within the ecosystem. Based on the results of this work, we provide a list of recommendations aiming to address the identified policy gaps and weaknesses.

1.2 Document Structure

The document includes the following chapters:

- Chapter 2 describes the cyberinsurance ecosystem including the main and secondary actors involved in the cyberinsurance processes, the relations between actors and their goals towards the adoption of cyberinsurance.
- Chapter 3 describes a framework of policy measures based on literature, analyses how the described policy measures map onto the main actors' goals, and discusses the identified policy gaps.
- Chapter 4 analyses how current cyber security regulations and directives concern cyberinsurance and the policy measures introduced in Chapter 3.
- Chapter 5 presents the results of an empirical study focusing on how cyberinsurance decisions sit in the broader ecosystem of cyber security and risk decisions at the company level.
- In Chapter 6 we report the results of a qualitative study with Dutch SMEs providing insights on what mechanisms and factors explain how SMEs decide on cyberinsurance adoption.
- Chapter 7 presents an agent-based model of the effects of different types of policy interventions on overall risk and discusses the finding of simulations based on this model.
- Chapter 8 concludes this document with a summary of our findings and a list of the final recommendations to EU and national-level policy makers.

2 Cyberinsurance ecosystem

This chapter provides an overview of the processes existing in the cyberinsurance ecosystem and the parties involved in those processes. This ecosystem description will serve as a basis for identification of possible gaps and limitations in the key directives and regulations that are not optimal for cyberinsurance adoption. We specifically focus upon the cyberinsurance ecosystem from the EU perspective because CYBECO is an EU project funded under the H2020 programme and aims at supporting EU policymakers. Therefore, most examples of regulatory authorities and directives are made for EU member states.

2.1 Cyberinsurance

According to Fauntleroy, "cyberinsurance is a risk transfer product that corporations can buy to mitigate losses due to information technology (IT) problems" (Fauntleroy *et al.* 2015). However, industrial practice shows that cyberinsurance covers losses mainly related to a virus or hacking attacks as well as data breaches rather than IT problems in general. Therefore, we define cyberinsurance as *a product for companies that would like to transfer the risks related to a virus, hacking attacks, and data breach events.*

Cyberinsurance involves at least two main parties: the insurance provider (*insurer*) and the *company* that would like to buy cyberinsurance. Once the latter purchase cyberinsurance it becomes an *insured* company. In many cases, companies work through an insurance broker who might advise clients on cyberinsurance offerings available on the market as well as help to negotiate a custom solution with a cyberinsurance provider.

Our overview of the cyberinsurance ecosystem is based on the literature on cyberinsurance and security risk management, analysis of major cyberinsurance products available on the market, and experience from our project partner within the insurance domain. We aimed to identify the main and secondary actors involved in cyberinsurance processes.

According to Marotta *et al.* (2017), the cyberinsurance life cycle includes the following processes:

- *Insurance offer request*. Once a company decides that it needs to transfer some residual risks and wants to buy insurance, it sends a request to an insurer.
- *Risk assessment*. The insurance provider (insurer) conducts identification and analysis of the company's risks. The approaches used at this step may vary upon the type of the company (SME, large corporation, medical hospital, etc.) and insurer's internal process. The insurer may a) use in-house security auditors, b) outsource risk assessment to a contracting audit company, c) conduct company profiling based on a security posture questionnaire (Romanosky *et al.* 2017)), or d) employ some technologies like machine learning or fintech (financial technology) solutions to do an informed underwriting.
- *Contract preparation*. As soon as the insurer has risk assessment results, they specify the coverage and decides upon the premium based on the available information.
- *Contract agreement*. The insurer sends the contract to the company (or its broker). Both insurer and company agree to the insurance contract conditions and sign it.
- *Insurance claim handling*. If an insured company has an incident, it notifies an incident manager about the problem and activates insurance policy. This process may involve

other parties like breach counsel to handle the problem, forensic investigator (e.g., police or private investigator) to study the incident, and the regulator that has to be notified about specific types of incidents. Based on the available information provided by the insured company and forensic investigator, as well as insurance contract conditions, the insurer decides the amount of compensation to be paid.

Figure 2.1 illustrates the part of the cyberinsurance life cycle from the insurance request that a company sends to an insurance broker, until the stage when the contract proposal is received. In this diagram, the insurer outsources the risk assessment to an external risk assessment provider. The insurer may also conduct security risk assessment of the potential client using security questionnaire (Romanosky *et al.* 2017) without involving external experts or use some technological solution, e.g., QuadMetrics[1], to assess company's cyber security level.

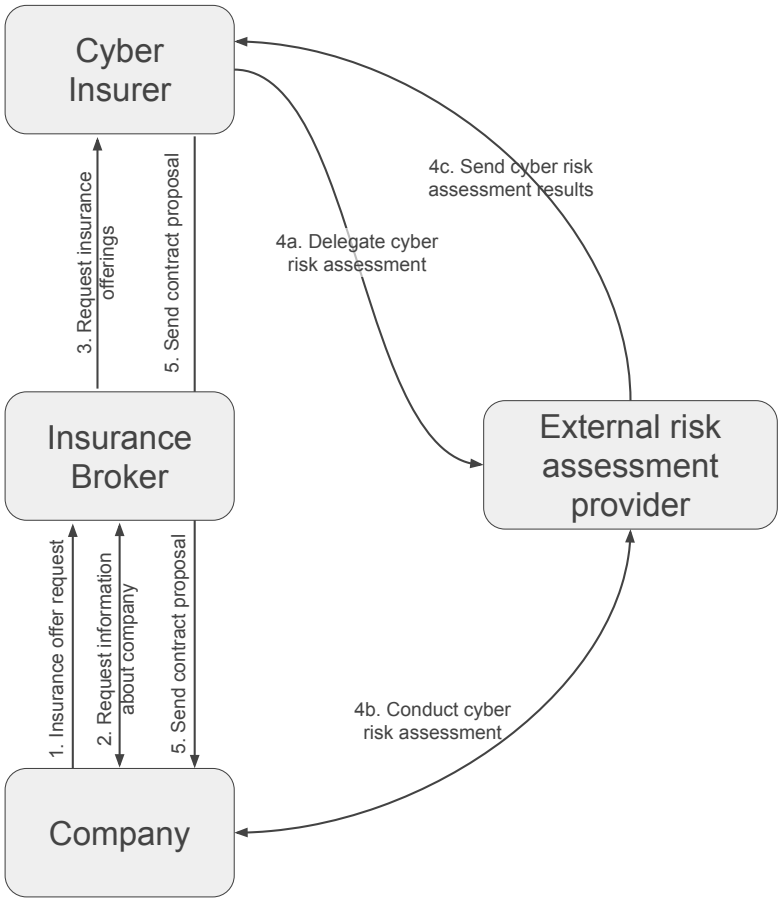

Figure 2.1: Cyberinsurance contract agreement process

Regarding the last step, "Claim handling", the incidents can be of different kinds depending on the type of the underlying cyber risk. Therefore, this process may vary between different cases. However, in most cases, this process starts with the first notification of loss (FNOL) when insured company notify an insurance manager about a security incident. The manager further connects the company with necessary service providers that specialize in cyber security, IT forensics, legal or PR questions.

[1] www.quadmetrics.com

2.2 Cyberinsurance actors and relationships

Knowing the cyberinsurance life cycle (see Section 2.1), we can identify the involved parties and the relationships between them (see Figure 2.2). We can also discuss the goals of the principal actors regarding the adoption of cyberinsurance.

2.2.1 Main actors

As discussed in Section 2.1, the main actors of the cyberinsurance are:

- *Insurance provider (insurer)* is "a party that assumes risks of another party in exchange for payment" (Marotta *et al.* 2017). The insurer has several goals within the ecosystem. First of all, it is a profitable portfolio of clients and a good level of market share. The main challenge for insurance companies is to propose adequate coverage for the client and ask reasonable premiums in return. At the same time, the insurer should carefully manage the transferred risks as it may face a cyber risk catastrophe when many clients in the insurer's portfolio are affected by the same threat. It may be controlled by suggesting that companies need to implement security countermeasures (this may be suggested through policy requirements and/or premium reduction). Other goals are a clear cyberinsurance policy and effective risk management of their insurer's portfolio.
- *Company* is an organization that would like to buy cyberinsurance. Once a company buys cyberinsurance it becomes *insured* company. In CYBECO the companies are divided into three main categories:
  - *SME group* includes companies with a staff headcount below 250 persons and a turnover $\leq$€50 million[2].
  - *Medium size companies* have a staff headcount below 2000 persons and a turnover $\leq$€500 million[3].
  - *Large companies* have a staff headcount more than 2000 persons and turnover $>$€500 million.

  With the adoption of cyberinsurance companies seek for 1) better understanding of the potential cyber risks, 2) cover possible losses related to cyber risks that company could experience in return for 3) reasonable premiums, 4) help in deciding on the investments in the most cost-effective security countermeasures, 5) handling after-incident process to help company to recover from the attack. We will investigate these goals in details in Chapter 6.
- *Insurance broker* is a party that advises companies on insurance products available on the market and matches companies' needs with appropriate insurance offerings. The goals of the intermediaries are somehow similar to the insurers' ones, namely a profitable business and successful matchmaking of companies to the available insurance products leading to better market penetration.

[2] http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_fr
[3] http://www.investopedia.com/terms/m/middle-market-firms.asp

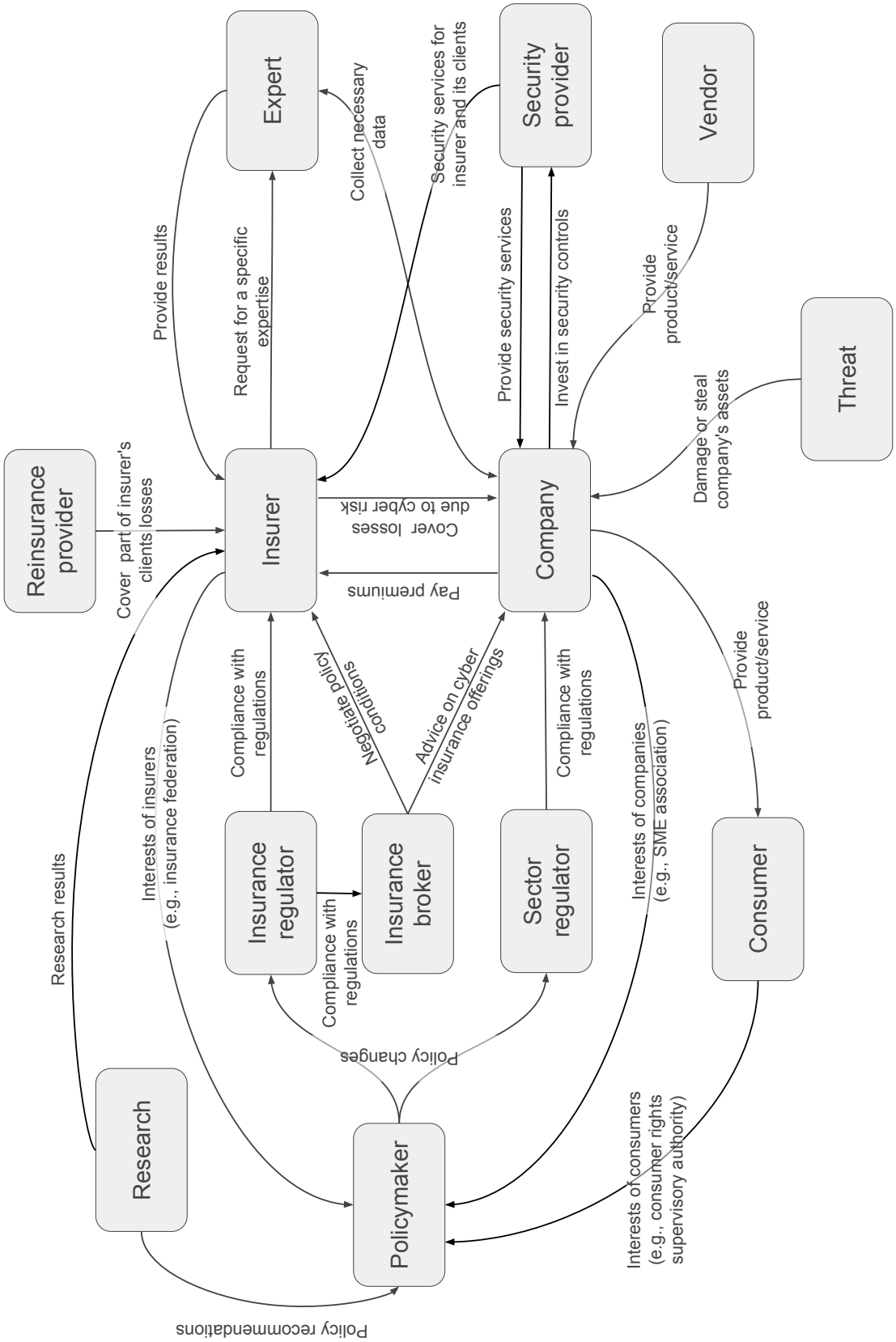

Figure 2.2: Cyberinsurance ecosystem

2.2.2 Secondary actors

In what follows we discuss the secondary actors that can be involved in the cyberinsurance life cycle (in alphabetical order):

- *Consumer* is an ultimate user of a company's products or services (Mentzer *et al.* 2001). The interests of consumers can be communicated to policymakers via research and authorities protecting consumers' rights (e.g., European Insurance and Occupational Pensions Authority). The main goal of the consumer is to get a high-quality product or service provided by the company in return for a cost. By high quality refers to the product or service satisfying the customer's needs (e.g., safety, security and privacy requirements).

- *Expert* is a party that provides different professional services (e.g., risk assessment, forensics, legal consultancy, etc.) that could be necessary to an insurer. Experts can be either employee of the insurer or external parties. The following service providers can be considered for the role of experts:

  - *Risk assessment provider* is a party that conducts an assessment of a company's security risks and provides the evaluation results to the insurer. Insurers can also have an in-house expert who performs the risk assessment of the companies. There are different ways of performing security risk assessment of a company. The primary approach is based on self-assessment security questionnaires (Romanosky *et al.* 2017). The more effort demanding process is to conduct a security risk assessment using one of the existing SRA methods (e.g., ISO 270001, NIST 800-30, CORAS, COBIT 5, etc.) Another option can be an evaluation of company's security profile using predictive models like QuadMetrics.

  - *Forensics provider* is a party that can be involved in the investigation of a security incident to discover what has been affected and how the consequences can be mitigated (AIG 2017), e.g., whether the information locked by a ransomware can be restored without paying a ransom; or find the cause of the incident before the claim will be reimbursed (Marotta *et al.* 2017).

  - *Breach counsel* is a party that assists a company "in understanding its legal obligations regarding evidence preservation, notification requirements and internal policy compliance" (Arant 2016).

  - *Legal and PR* is a party that provides legal advice and PR consultancy to minimize damage to reputation (AIG 2017).

- *Policymaker* is an organization or individual who participates in the process of policy making, e.g., national government, members of parliament, special national government organizations, etc. Policymakers rely on the information from different parties like researchers, lobbyist, insurance or SME associations, analytical organizations, and others[4]. Once the policy is created or updated it passes to a regulator that is responsible for its implementation.

  The primary goal of the policymaker from the national perspective is to improve the overall level of security. To achieve this goal the policymakers are also interested in motivating

[4]UN Food And Agriculture Organization, "Communicating with policymakers" `http://www.fao.org/docrep/014/i2195e/i2195e02.pdf`

companies to implement a minimal set of security countermeasures through the requirements of cyberinsurance policy.

- *Reinsurance provider (re-insurer)* is a party that assumes part of the risk covered by other insurers in exchange for payment. Reinsurance can be considered as insurance for insurers (Kesan & Hayes 2017). The re-insurer can be a private organization (e.g., Munich Re[5]) or a government (Robinson 2012).

- *Regulator* is a "public organization that is involved in rulemaking and can also be responsible for investigation or audit, monitoring, dispute decision, and enforcement" (Levi-Faur 2011, Ch. 1, p.11). Companies can be regulated by different authorities depending on their business sector. Our primary interest is the cyber risk and, therefore, we focus mostly on the cyber risk related regulators and regulations, for example:

  - *National Data Protection Authority* who is responsible for monitoring the compliance with data protection law within its country (e.g., General Data Protection Regulation in EU). Companies who work with personal data, have to comply with data protection law (e.g., GDPR) and will be controlled by a Data Privacy Regulator (e.g., Dutch Personal Data Protection Authority (in Dutch: "Autoriteit Persoonsgegevens") or French Data Protection Authority ("Commission nationale de l'informatique et des libertés")).
  - *The Directive on security of network and information systems* (NIS directive). Many companies rely on networks and information systems (IS) as well as provide services to their customers. Thus, they have to be compliant with the NIS directive and ensure a high level of security of their networks and IS to prevent cyber security incidents adequately. As a regulatory authority for this directive we can name French Networks and Information Security Agency[6].
  - *Domain-specific regulators*. For example, the growing IoT market can be subject to safety regulations as security incidents on physical devices may be hazardous to the health and life of consumers. For example, at the EU level non-food products should be compliant with General Product Safety Directive, and Consumer Protection and Technical Regulatory Authority is responsible for monitoring the implementation of this directive in Estonia.

  Insurance companies have to deal with the following regulators and regulations

  - *NIS and GDPR*: Insurance companies work with personal data of their clients and, therefore, have to be compliant with data protection law. The NIS directive is also applicable to insurance providers as they use networks and information systems and support their clients with various information services.
  - *Central Bank* who ensures that insurance providers can pay client's claims. Bank of England[7] or De Nederlandse Bank[8] can be examples of that regulators.
  - *Financial Services Regulatory Authority* who supervises insurance companies to ensure fair treatment of customers and transparency of insurance services. For

[5] https://www.munichre.com
[6] French: Agence nationale de la sécurité des systèmes d'information (ANSSI). https://www.ssi.gouv.fr/en/mission/audiences-and-activities/
[7] https://www.dnb.nl/en/statistics/statistics-dnb/financial-institutions/insurers/index.jsp
[8] http://www.toezicht.dnb.nl/en/4/5/12/51-204674.jsp

example, Netherlands Authority for the Financial Markets[9] or Federal Financial Supervisory Authority in Germany[10]

– *Insurance regulator* protects public interests, promotes competitive markets, and facilitates fair treatment of insurance consumers. For example, in EU the insurance regulator is Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS)[11] and National Association of Insurance Commissioners (NAIC)[12] in the US.

- *Researchers* is a party that investigates cyberinsurance in a systematic way. Research results can serve as an input for insurance companies and policymakers. Research is also crucial for the evaluation of the effect of the policy changes.

- *Security provider* is a party that provides security solutions to another party to protect their assets. It can provide security solutions and services directly to companies or in a partnership with insurers.

- *Threat* is "an event with the potential to adversely impact organizational operations (incl. mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" (Kissel 2013).
From the perspective of CYBECO, aspects like motivation and intention of a threat could be important components for understanding the behavioral part of an attack. From the modeling perspective, it is important to consider insider and outsider threats. If the goal of the attacker is stealing information, then the outside attacker needs to get access to company's information system (or premises) to achieve its goal, while an insider does not need this step.

- *Vendor* is a party that supplies companies with a product or service. It can be a network provider or vendor of software that is necessary for company's business processes. In turn, the company can play the role of the vendor for other companies (Mentzer *et al.* 2001). The regulatory compliance may be extended from the company to its vendors, e.g., a company may require its vendors to have cyberinsurance or demonstrate compliance with directives like NIS, GDPR or domain-specific regulations.

2.3 Goals of the main actors

In October 2017 - May 2018 we conducted a series of interviews with representatives of insurance providers, brokers, SMEs, and government. During the interviews, we discussed the proposed ecosystem model and the primary goals of the corresponding actors towards the adoption of cyberinsurance.

[9] Dutch: Autoriteit Financiële Markten https://www.afm.nl/en/over-afm/werkzaamheden/strategische-doelstellingen

[10] https://www.bafin.de/EN/Aufsicht/VersichererPensionsfonds/versichererpensionsfonds_node_en.html

[11] https://eiopa.europa.eu/regulation-supervision/insurance

[12] http://naic.org

2.3.1 Insurance provider

An insurance provider is interested in increasing their market share, having better actuarial data to improve risk assessment and run a profitable business. An insurance company representative is quoted: “we think it is a big market, a big piece of cake and we would like to take a piece of it. With good underwriting, we may also have profit on it. But you never know because it is new.”

2.3.2 Intermediary

An insurance broker aims at making a profit, but also at providing their clients with high-quality advice about cyber risks. As stated by a broker representative, their main goal is “to provide all my customers with a cyber policy. I want all my customers to make a decision about it, how to solve this. [. . .] To be 100% conscious about the risk and made decisions they are aware of.”

2.3.3 SMEs

Companies try to get advice on security investments, cover possible losses related to cyber risks, and in case of an incident to get help with incident handling. A typical statement in this regards is that “if something happens, the way they help with the process, what should we do, where to go. This is one of the reasons why we get it because we do not know much about it and they do.”

2.3.4 Policymakers/Government

At a higher level, we have a regulator or government actor whose primary interests are to increase the overall level of security and create a resilient ecosystem (PwC, 2017). In the discussion, a government representative from Luxembourg mentioned that their “goal is to improve the overall level of security in Luxembourg.” Cyberinsurance is considered as a way to “increase the number of people that are active in this cyber security ecosystem.”

2.4 Conclusion

This chapter presented the cyberinsurance ecosystem that describes the main actors involved in the cyberinsurance process, in addition to other actors indirectly involved in the process. We also identified the goals of the main actors towards the adoption of cyberinsurance. In the following chapters, we will use the introduced ecosystem as a basis for analysis of existing regulations and identification of required policy recommendations.

3 A framework of policy measures and cyberinsurance

Current cyber security regulations and standards are limited in regards to cyberinsurance. Therefore, we adopted a framework proposed by Woods & Simpson (2017) to identify possible policy measures that can be considered by the policy makers for improving the cyberinsurance market. The framework provides six main themes of possible policy measures: wider adoption, defining coverage, data collection, information sharing, best practices, and catastrophic loss. In this chapter, we describe these themes and related policy measures, link them to the goals of the actors in the cyberinsurance ecosystem as well as ethical considerations, and identify missing elements.

3.1 Framework of Policy Measures for Cyber Insurance

3.1.1 Wider adoption

This theme covers policy measures related to expanding the adoption of cyberinsurance among organizations. A larger pool of clients who insure themselves against possible cyber damage can be seen as a utilitarian justification for social welfare and redistribution.

The first policy measure contributing to this theme is *legislation assigning financial costs to cyber events*, e.g., regulatory fines. The US market has already experience with the adoption of similar policy measures in 1996 with Health Insurance Portability and Accountability Act (HIPAA) when the technology-centered insurance was in its infancy and, later, in 2003 with California Data Breach Laws when the companies became obliged to notify parties affected by a data breach that the organization has suffered. These policy measures caused a huge growth in the US cyberinsurance market (US DHS 2012).

Another policy measure that could contribute to the wide adoption of the cyberinsurance is *raising awareness that traditional insurance policies do not cover cyber risk*. In many cases, insured companies blindly believe that cyber risk is covered under traditional insurance policies like property, general liability, directors and officers liability, errors and omissions liability, and others (OECD 2017a). Thus, it is important to educate companies and raise their awareness regarding the problem of “silent” coverage of cyber risk in traditional insurance policies. The government could also “support the development of cyberinsurance market via governmental procurement capability”. Specifically, the governmental agencies could be encouraged to buy cyberinsurance themselves, e.g., for critical infrastructure and critical services (Marsh March 2015) or could include cyberinsurance in the list of requirements for organization participating in government tenders (US DHS 2012).

The last policy measure from this set is *making cyberinsurance mandatory for specific business sectors*; similar to healthcare or car insurance, cyberinsurance could also be an option for certain business areas. However, this would require a thorough analysis of the effects and consequences for the corresponding organizations and the market itself. Research on possible mandatory flood risk insurance in the Netherlands showed that this would result in an inefficient ecosystem (Kok *et al.* 2002). The resulting risk premium could better be invested in structural measures to reduce the flood risk, mainly caused by the fact that flooding in the Netherlands causes damage to a large number of objects simultaneously (so-called dependent failures). This is in contrast to for instance fire insurance, where the fires in objects are independent events.

3.1.2 Defining coverage

Defining coverage theme includes policy measures related to development of common and clear terminology for cyberinsurance policies. First of all, the market should develop a *standard language for cyberinsurance policies* that will help all ecosystem actors to have a clear understanding of what is covered under a certain insurance policy. At the same time, insurers have to *promote the use of cyber exclusion clauses in non-cyber policies* to cope with the problem of "silent" coverage and increase corresponding awareness among their clients. In this way, companies will think about standalone cyber products if they see that cyber is not in their traditional insurance. Finally, the cyberinsurance market requires a *certification of cyber war or terrorism acts provided by the government* as more often we deal with cyber attacks that are created by state actors. For example, Zurich Insurance Group has recently rejected the claim by Mondelez to cover the losses that the company suffered due to NotPetya ransomware attack. Zurich was since added an exclusion for "hostile or warlike action in time of peace or war" (Bershidsky 2019).

3.1.3 Data collection

This theme comprises of the policy measures aimed at improving data collection practices. The first proposed measure is related to the introduction of *standard data formats for risk assessment and claim processes*. Most insurers use their own questionnaire(s) to collect information about organization level of risk. There are several initiatives offering market actors free to use tool helping companies identify the relevant cyber risks and their preparedness to cyber incidents like Cybersecurity Assessment Tool by Federal Financial Institutions Examination Council (FFIEC)[1] or Monarc Risk Assessment Method and Platform developed by SECURITYMADEIN.LU[2]. These tools can serve as a basis for the development of standardised proposal forms. The next proposed policy measure is related to setting *minimum requirements for risk assessment data collection*, so to limit cases when insurers provide contracts to companies without a clear idea about their level of cyber security preparedness. Finally, regulators should improve the *collection of high-level data on the cyberinsurance market* in order to understand the current trends at the market and level of penetration for cyberinsurance.

3.1.4 Information sharing

This set of policy measures relates to making collected data available to a wider number of ecosystem actors. One of the sources of valuable data for cyberinsurance is *information collected by government agencies*. However, making this data available is a sensitive topic as it may be related to national security matters. Another data source is providing *open access to sector-specific information-sharing initiatives* (sector ISACs).

New EU cyber security directives (e.g., GDPR and NIS) have recently come into force and regulators collect a significant amount of data related to the data breaches and cyber security incidents. In this regard, there is an ongoing discussion around *making available data collected by government agencies* under these directives[3]. Having this data could help insurers with a limited number of claims to improve their actuarial models and offer clients better cyberin-

[1] https://www.ffiec.gov/cyberassessmenttool.htm

[2] `https://www.monarc.lu/`

[3] Insurance Europe. More must be done to address the lack of information on cyber attacks `https://www.insuranceeurope.eu/more-must-be-done-address-lack-information-cyber-attacks`

surance products. The other ecosystem actors could also benefit from the *"extended public disclosure of data breaches"* that helps with generating *"a complete picture of the costs and benefits of cyber security investments"* as suggested by Nieuwesteeg *et al.* (2018a).

All these policy measures could be the basis for creating a *government level cyber incident data repository*. This repository could aggregate information from individual organisations and government agencies. However, before this can become a reality, we need to solve challenges related to the anonymisation of collected data for protecting national security and limiting probable reputation damage to organisations.

3.1.5 Best practices

This group of policy measures tackles cyber security risk management practices. Some ecosystem actors consider cyberinsurance as a tool for improving the overall level of cyber security through introducing minimum requirements to security countermeasures within cyberinsurance policies. Thus, governments should create a *standard in information security best practices* that insurance providers could use as a baseline for risk assessment and as a *basic level of security requirements from companies seeking insurance*. Numerous cyber security best practice standards exist in the world like ISO27002, NIST 800-53, BSI IT-Grundschutz catalogues, Cyber Essentials, and others. However, there is no agreement on which one is better to use for cyberinsurance needs. There are some cyber security certification initiatives at the EU and national levels. For example, in 2018 Dutch ministry of Justice & Security funded a three-year project aiming at developing a quality mark and certification scheme for cyber risks fitting the needs of SMEs. The project involves cyber security experts, an association of entrepreneurs, involves insurers, and other stakeholders. At the EU level, there is the European Cybersecurity Certification Group within the European Cyber Security Organization. As suggested by Cihon *et al.* (2018), this group could *"engage with industry stakeholders in order to draft guidance on the use of cybersecurity certification to meet a firm's cybersecurity duty of care [...and] coordinate "*.

Another policy direction is that regulators should clearly explain the *role and liability of insurance providers in advising their clients on cyber security*. The insurance providers should look for a balance between the desire to sell cyberinsurance products to companies and requiring a minimal level of cyber security from them (in case of low security level).

3.1.6 Catastrophic loss

The final group includes policy measures targeting catastrophic loss events (e.g., terrorism). The main policy measure that is discussed within this category is *the role of government as re-insurer of last resorts*. Woods & Simpson (2017) discussed two approaches used in the U.S. (TRIA) and the U.K. (Pool Re) and how they differ. The main differences are related to 1) funds collection ex-ante (Pool Re) or ex-post (TRIA), 2) premium pricing according to underlying risk (Pool Re) or the amount of sold insurance policies (TRIA), 3) optional (Pool Re) or mandatory membership (TRIA). Another policy option that should be taken into account is an *upper limit on the amount covered by the scheme* for one loss event or, alternatively, an *upper limit on the amount that each insured can claim* Brice (1994). A detailed discussion can be found in Woods & Simpson (2017, p.12).

3.2 Mapping of policy measures on ecosystem actor goals

To further understand which policy measures have more influence on the ecosystem and whether there are any gaps, we mapped the goals of the actors from Section 2.3 to the themes of the framework. Table 3.1 provides an overview of how actor's goals are mapped onto policy measure groups from Woods and Simpson's framework.

Wider adoption of cyberinsurance is linked to the growth of the market and, therefore, supports goals like increasing market share for insurers, making a profit for insurers and brokers. At the same time, wider adoption means that more companies insured their cyber risks, implying that the resilience of the ecosystem is also increasing.

Policy measures related to *coverage definition* help brokers to better advice companies about relevant insurance products meaning that companies get an appropriate policy to cover their cyber risks. Wider use of cyber exclusions in non-cyber policies could lead to improving the level of sales of cyberinsurance products contributing to the profitability of insurers and brokers.

Data collection policy measures impact upon insurers' goal related to having better actuarial data. For other actors' goals this policy measure does not have a direct connection.

Information sharing measures also supply insurers with actuarial data and help brokers to provide clients with high-quality advice regarding cyber risks, as brokers can have real information about current cyber incidents.

Security best practices measures help brokers to advise their clients on cyber risks and countermeasures, meaning that companies get advice on what security investments to make. By using *security standards* in cyberinsurance risk assessment and even including security best practices as required in a cyberinsurance policy, the government could affect the overall level of security in the ecosystem.

Catastrophic loss measures contribute to the increase of ecosystem resilience which is the goal of the governmental actor.

The only goal that is not covered by this policy measures framework is related to company actors who need assistance in incident handling. However, the existing practice shows that most insurers offer their clients crisis management service as a part of cyberinsurance products. Mostly this service provided by partnering organisation which costs are included in policy coverage (Romanosky *et al.* 2017, Nieuwesteeg *et al.* 2018b). It is probably that we need to take this policy gap into account and support more close collaboration between cyber incident handling initiatives like CERTs and cyberinsurance providers. Governments could facilitate this relationship at the policy level.

Table 3.1: Mapping of policy measure themes on ecosystem actor goals

	Goal	Wider adoption	Defining coverage	Data collection	Information sharing	Best practice	Catastrophic loss
Company	Get advice on security investments					X	
	Cover possible losses related to cyber risk		X				
	Help with incident response						
Broker	Provide high quality advice about cyber risks		X		X	X	
	Make profit	X	X				
Insurance provider	Increase market share	X					
	Have better actuarial data			X	X		
	Profitable business	X	X				
Regulator/ government	Increase overall level of security					X	
	Resilient ecosystem	X					X

3.3 Ethical considerations

Ethical considerations are important in an insurance context because insurance arrangements reshape responsibilities in addition to redistributing risk (Baker 2002, Doyle 2011). This means that the policymaker aiming at influencing insurance arrangements has to take into account the impact of policy on such reshaping as a moral (and political) actor. “Although insurance tends to displace social control from the political to the administrative, questions about system design bring insurance back into the political realm” (Heimer 2003).

These ethical questions of responsibility have to do with the decision-making options that are made available to the different actors by the chosen arrangement. For example, insurers get to set availability and prices for different (potential) customers, and potential customers may get the option to buy insurance rather than taking other measures. Whether customers take other measures may in turn have influence on other individuals or common goods.

In this context, there are three key ethical questions:

1. Do insurance arrangements lead to moral hazard, i.e. the insured increasing their risk after purchasing insurance?

2. Do insurance arrangements undermine responsibility for collective goods/values, or are policymakers in any way unduly redistributing their own responsibility for those collective goods/values?

3. Are insurance arrangements fair with respect to effects of selection and premium differentiation?

In the following, we investigate how these considerations play out in the specific case of cyberinsurance, and what the implications are for policy-making in this domain.

First of all, cyber security is (at least partly) a setting of adversarial risk: in case of an incident, there may be someone who benefits (i.e. the attacker or perpetrator). This is similar to burglary events in the physical world. In such cases, part of the damages that are being paid by the insurer ends up in the hands of the perpetrator. Since financing a criminal business case is generally seen as undesirable, attention needs to be paid to the extent to which the availability of the insurance arrangements does not increase the attractiveness of the criminal activity, e.g. through weakening the investment in prevention (but instead correcting the negative outcome for the victim). Thus, whereas moral hazard is an ethical consideration in any insurance domain, security adds the additional concern that customers increasing their risk because of the availability of insurance generate revenue for the threat agents that are the source of the risk.

The value of security thus represents the protection of systems against such threat agents. The goals of security engineering (Pieters 2019) lie in developing (socio-technical) systems that contribute to security, or at least do not deteriorate the security situation. The main question is whether such security constitutes an individual value (the individual being protected against adversarial risk), or a collective value (a group being protected against adversarial risk). A key consideration in this respect is whether security measures taken by individuals contribute to the overall security of the group. This is indeed the case, because (a) increased security prevents infrastructure being used in other attacks, and (b) sufficient security protection by sufficient individuals weakens the business case for criminal activity (because it won’t scale). In this sense, security controls contribute to “herd immunity”, much like in the case of vaccination of people.

Therefore, security is at least partly a collective value. The problem with such collective values is that leaving the protection to individual decisions may lead to socially suboptimal decisions, because the effects on others (externalities) are not necessarily factored into the decisions. In this context, several authors have pointed to various notions of a "digital commons" (Anderson 2001, Greco & Floridi 2004, Regan 2002). The question is whether such collective goods/values can be sufficiently protected under a regime where individual (insurance) decisions play a key role.

Apart from the externalities associated with collective values, leaving security decisions to individuals and individual organisations can be problematic in other respects. In particular, (small) organisations may not have the required expertise, and advice given to them may be contradictory. They may lack the information and decision-making capacity to make good decisions even on individual risk. In this context, individualising risk has been criticised before under the term "responsibilisation" (Renaud *et al.* 2018).

When implementing policy decisions regarding cyberinsurance, a key question is therefore to what extent such policies individualise or responsibilise cyber risk, and whether such allocation of responsibilities is desirable. In particular, the main question is where the decision-making regarding cyberinsurance, and the associated responsibility, is allocated. If left to the market, individual organisations make purchase decisions, but these may not be optimal from a societal point of view. A comparison can be made with different regimes regarding health insurance in different countries. Policies regarding cyberinsurance can not be seen apart from key governance regimes in terms of responsibilities of states, market mechanisms, and individual responsibility. At one extreme, over-regulating may be seen as paternalism, for example, when specific controls or forms of insurance are made mandatory. At the other extreme, leaving everything to the market may be seen as dodging responsibility, and failing to create incentives for responsible behaviour by other actors.

An additional policy question is which forms of premium differentiation are seen as acceptable. This involves both questions of fairness and solidarity (Minty 2018, Palmer 2007), in the sense that people aren't punished for risks that are beyond their control, and questions around the means by which differentiation decisions are made, for example forms of data gathering. In cyberinsurance, the latter issue is more prominent, because risks are in principle controllable (unlike in health insurance). On the other hand, how the risks of individual customers are determined can be a source of controversy. For example, if premium differentiation is based on more than self-assessment, should customers provide access to auditors or even automated monitoring tools? To what extent is this a win-win between the customer and the insurance company, where the customer also learns about their risk and effect of controls, and to what extent does this create information asymmetry, where insurance companies are the only actors with a good picture of cyber risks and the effect of controls? And how do policy makers ensure access to relevant aggregated information about aggregated risk? When deciding on different policy options, policy makers should take into account the interconnectedness of differentiated premiums, data extraction, and the availability of data to key stakeholders (including policy makers themselves).

Finally, the issue of correlated risk is a key feature said to differentiate cyber risk from other insurable risks. Because victimization does not only depend on individual characteristics, but also on characteristics of computer systems used by many van der Wagen & Pieters (2019), a single event may affect a huge part of the insured population. On the one hand, addressing correlated risk via insurance mechanisms may involve societal risk, in the sense that coverage may not be guaranteed in case of worldwide damages. On the other hand, insurers will have

an incentive to address correlated risk, for example by stimulating developments that may provide security under radical technological changes (e.g. quantum computing), or encouraging diversity as opposed to monocultures of software (Pieters 2018).

These ethical considerations may have impact on the evaluation of the different policy options outlined in this chapter. *Wider adoption* of cyberinsurance, if not accompanied by other measures, may enhance criminal business case via moral hazard, because insecure companies may lack incentives for investment in security when they are insured. Although the CYBECO experiments do not show a strong moral hazard effect, this would need to be monitored in real-life circumstances. Efforts in defining coverage may also improve fairness of insurance, by explicating insurance conditions and making them understandable to the customers. For *data collection*, ethical considerations have to be taken into account regarding which forms of data collection are acceptable. More data may not always be better, and the feasibility of anonymisation needs to be considered. *Information sharing* can be used as a policy option to avoid the development of structural information asymmetries, created by large-scale data collection. *Best practices* can reduce moral hazard by fixing minimum protection levels. Finally, *catastrophic loss* can be addressed not only by reinsurance but also by investment in preparation for radical changes in the cyber security landscape. The latter may be better in terms of resilience and pro-active responsibility for the future.

In short, besides impact on the goals of the stakeholders, ethical considerations form an additional criterion against which to evaluate policy options.

3.4 Conclusions

This chapter presented the policy measure framework and how the identified measures are mapped on the goals of the main players of cyberinsurance ecosystem. We also discussed the main ethical questions that should be considered along with policy measures for cyberinsurance. The main conclusions of this chapter are:

- Woods & Simpson introduced a comprehensive framework of policy measures for cyberinsurance which covers most of the goal of cyberinsurance ecosystem players.
- The proposed policy measures covered most of the goals of the main actors in the cyberinsurance ecosystem. However, the goal of a company actor who needs assistance in incident handling is missing. The relations between companies and incident management providers (including those recommended by cyber insurers) are not defined at the regulation level.
- Policy makers have to take ethical consideration into account when evaluating possible policy measures.

4 Cyberinsurance in current cyber security directives and standards

The previous chapter discussed policy measures and their mapping to stakeholder goals. In this chapter, we review the existing regulations and directives related to cyber security and data privacy on how they concern cyberinsurance and the policy measures framework. The list of relevant regulations and directives with description is reported in CYBECO D4.2. For this chapter we investigated English documents or their translation to English in case of national regulations. For the IT Security Act (ITSiG) from Germany we could not find an English translation and therefore this was excluded from the review.

We have identified the two main areas of policy measures from the framework that are considered to a certain extent in the investigated regulations and directives. These measures are related to *legislation assigning financial costs to cyber events* ("Wider adoption" group) and *requiring certain level of cyber security from organizations* ("Best practices" group).

4.1 Wider adoption: legislation assigning financial costs to cyber events

Most of the reviewed regulations and directives contain clauses imposing penalties and fines in case of breach or incident events. Some regulations specify precise limits for fines, e.g.:

> "In case of a first breach, the penalty may not exceed €150 000. In the event of a second breach within five years from the date on which the preceding financial penalty becomes definitive, it may not exceed €300 000 or, in case of a legal entity, 5% of gross revenue for the latest financial year, within a maximum of €300 000." by *French regulation: "Act No. 78-17 of January 6 1978 on Information Technology, Data Files and Civil Liberties".*

The other examples of specific financial penalties can be found in:

- "Regulation 2016/679 - General Data Protection Regulation" (GDPR) from EU in Article 83 (4) which sets fines limits at *"up to €20 000 000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher"* for violation various conditions including data processing principles along with appropriate security measures for protecting personal data (see Article 5f).

- "Federal Data Protection Act" from Germany refers in Section 41 to the GDPR regulation in relation to the size of financial penalties and in the next sections the regulation specifies for which actions are applicable penal provisions (Section 42) and administrative fines (Section 43).

- "Special Data Protection Act 1999" from Spain sets fine ranges in Article 45 on Penalties. The new "Organic Law 3/2018" that has been adopted in Spain to implement GDPR directive at the national level on December 5, 2018. The new law refers to Article 83 of GDPR in relation to the possible sanctions for law breach.

- the UK "Data Protection Act 1998" did not define financial penalty limits, but in the new "Data Protection Act" adopted in 2018, there is section 157 setting the maximum amount of penalty in line with Article 83 of GDPR.

We did not find information about specific financial penalty ranges in the "Federal Act on Data Protection" adopted in Switzerland. In the EU "Directive 2016/1148 - Network and Information Security (NIS) Directive" also does not define financial penalty ranges, but require Member States to "lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to the Directive and shall take all measures necessary to ensure that they are implemented."

4.2 Best practices: requiring certain level of cyber security from organizations

The proposed policy measure on *requiring certain level of cyber security from organization* in relation to cyberinsurance means setting a certain level of security requirements as part of cyberinsurance product. We also investigated what security requirements are required by existing cyber security regulations. Some directives provide general requirements regarding security measures:

- **Switzerland**, "Federal Act on Data Protection" in Art. 7 on Data security:
  "1) Personal data must be protected against unauthorised processing through adequate technical and organisational measures.
  2) The Federal Council issues detailed provisions on the minimum standards for data security."

- **EU**, NIS directive in Article 14 on Security requirements and incident notification: "Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed."

- **EU**, "Data Protection Directive 95/46/EC" in Paragraph 46: "Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;"

The other part provides more details on what security aspects should be considered by responsible parties:

- **Spain**, "Special Data Protection Act 1999" in Article 9 on Data security:"The controller or, where applicable, the processor shall adopt the technical and organisational measures necessary to ensure the security of the personal data and prevent their alteration, loss, unauthorised processing or access, having regard to the state of the art, the nature of the data stored and the risks to which they are exposed by virtue of human action or the physical or natural environment."

- **France**, "Act No. 78-17 of January 6 1978 on Information Technology, Data Files and Civil Liberties" in Article 34: "The data controller shall take all useful precautions, with regard

to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties."

The most detailed requirements regarding security we found in the following regulations:

- **EU**, GDPR in Article 32 on Security of processing: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
  (a) the pseudonymisation and encryption of personal data;
  (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

- **Germany**, "Federal Data Protection Act" in Section 22 on Processing of special categories of personal data (part (2)): "[...] appropriate and specific measures shall be taken to safeguard the interests of the data subject. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:
  1. technical organizational measures to ensure that processing complies with Regulation (EU) 2016/679;
  2. measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
  3. measures to increase awareness of staff involved in processing operations;
  4. designation of a data protection officer;
  5. restrictions on access to personal data within the controller and by processors;
  6. the pseudonymization of personal data;
  7. the encryption of personal data;
  8. measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
  9. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
  10. specific rules of procedure to ensure compliance with this Act and with Regulation (EU) 2016/679 in the event of transfer or processing for other purposes."

- **UK**, Data Protection Act 2018 in Article 66 on Security of processing: "(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data.

(2) In the case of automated processing, each controller and each processor must, following an evaluation of the risks, implement measures designed to —
(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it, (b) ensure that it is possible to establish the precise details of any processing that takes place,
(c) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and
(d) ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions."

4.3 International standard for cyberinsurance

ISO and IEC organizations are currently developing a new standard defining information security management guidelines for cyberinsurance (ISO/IEC DIS 27102) (ISO/IEC 2019). This standard aims at providing guidelines for adoption cyberinsurance as one of risk mitigation strategies that help to manage the financial consequences of a cyber incident on the organization. However, this standard is at the earlier stages of the development and requires attention and contribution from different stakeholders to address goals of the main ecosystem parties (see Section 2.3) and limit possible adverse effects from its introduction.

4.4 Conclusions

Most of the studied regulations define the ranges for financial penalties except EU NIS and Swiss directives, which probably require additional attention from policymakers side. Concerning policy measures requiring a certain level of security from organizations, we found out that there is no agreement on the level of details of security requirements across existing cyber security regulations. The tendency of making security requirements more general can be explained that the legislation needs to take into account the changing nature of cyber security risks and new developments in the area of cyber security protection. The GDPR and German directives can be considered as examples of legislation with the most detailed security requirements while NIS directive and "Federal Act on Data Protection" from Switzerland are the least detailed in these terms. However, what is an appropriate level of security requirements is still an open question and needs more attention from cyber security and policy analysis research.

5 Empirical investigation of policy usability

Whilst the previous chapters have looked at the cyberinsurance ecosystem and associated policy measures, in this chapter we focus upon how cyberinsurance decisions sit in the broader ecosystem of cybersecurity and risk decisions at company level. In particular we are interested in unpacking the role of the company as an actor within this ecosystem (Figure 5.1), in order to understand better how policy measures may affect company decisions.

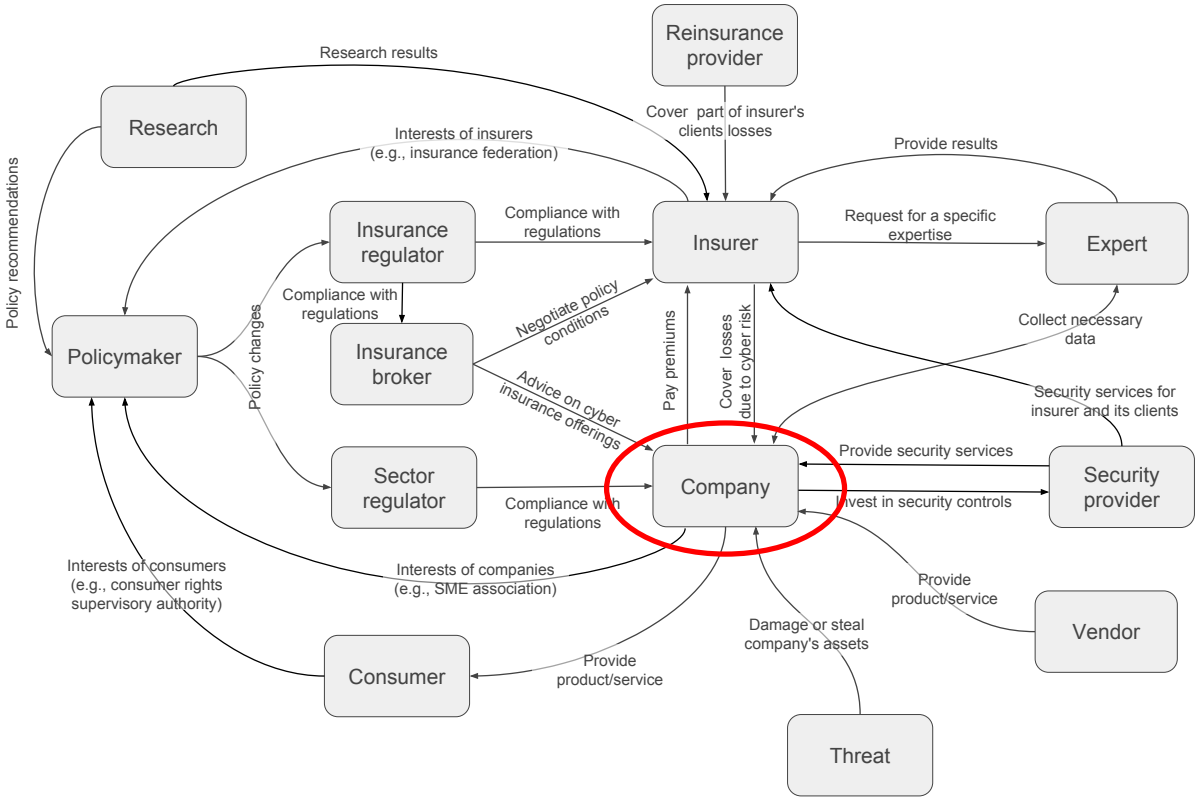

Figure 5.1: Focusing upon the company within the cyberinsurance ecosystem

5.1 Background

Research has been conducted into how decision-makers determine which security products to purchase, but there is little understanding of the processes involved prior to the purchasing stage, e.g., who is responsible for making cybersecurity decisions (organising staff training, policies, purchasing)? This information is vital to assess the usability of current policy. Companies must make key investment decisions around security measures (including cyberinsurance) on a regular basis, however there is a lack of research directly investigating how companies make these decisions (as identified by Weishäupl *et al.* (2018)). A recent literature review by Heidt *et al.* (2019) highlighted that there is a scarcity of studies analysing IT related security decision-making from a behavioural, environmental and organisational perspective, thus arguing that consideration of contextual factors influencing IT security decisions is vital ((Heidt *et al.* 2019, p.6145)). They also argue that the majority of research in this area is quantitative in

nature and can miss these contextual factors.

It is important to recognise that companies contain a complex ecosystem in their own right – and that this complexity is likely to vary considerably between smaller companies (i.e., SMEs) and larger companies. Therefore the study reported in this section expands upon our previous work by exploring a wider range of companies including very large organisations.

The Burke & Litwin (1992) Change Model demonstrates some of the complexity of attempting to model processes within companies (Figure 5.2). The model illustrates how behaviour within companies can be influenced by a complex system of twelve different factors. All of the pathways between the factors are bidirectional, and therefore all of the factors from company structure, to motivation in the workplace can feed into organisational change in many different ways.

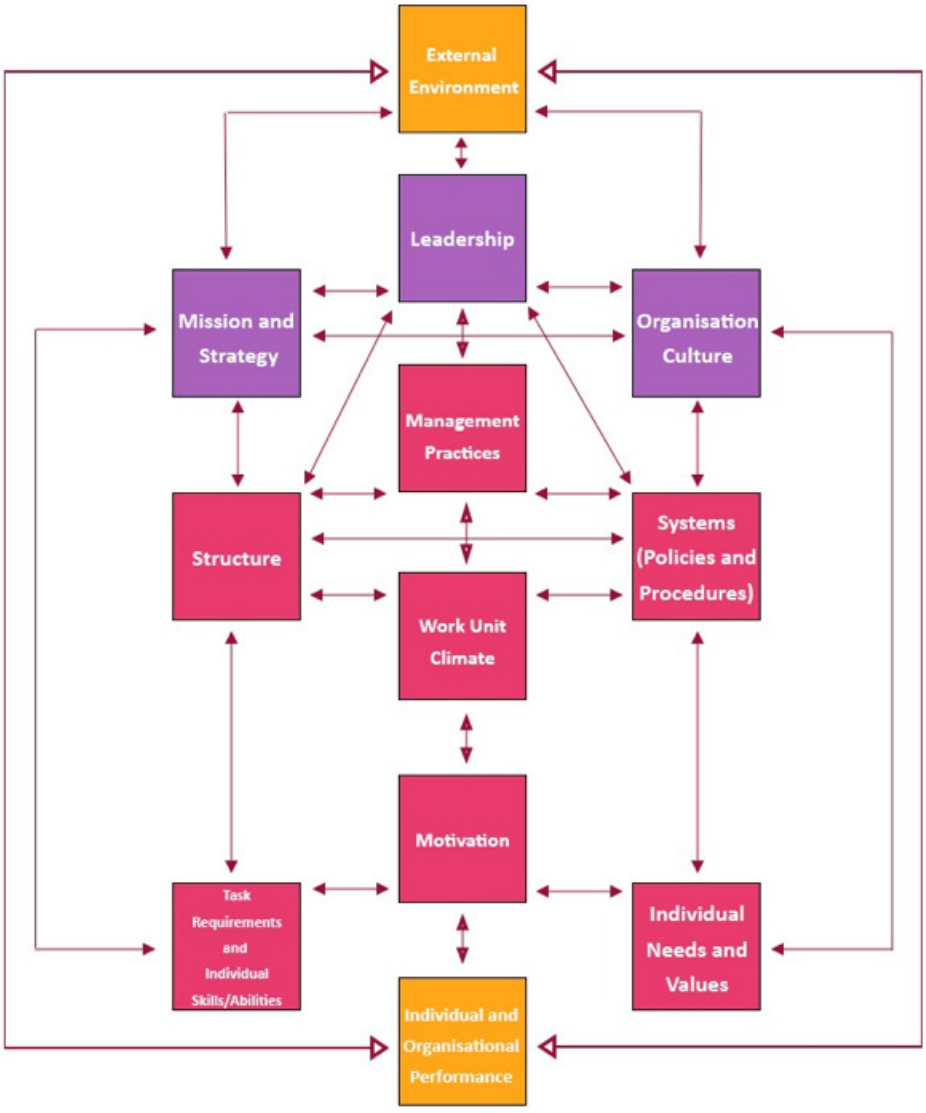

Figure 5.2: Burke and Litwin Organisational Performance and Change Model

Type of business experience	Number of interviewees
Experience in both SME & Large Companies	3
SME experience only	1
Large company experience only	2
Insurer/Broker/Consultant	5

Table 5.1: Interviewee experience/background

The most dominant factor in the model is the external environment. It is through this change that a company will change its mission, culture, leadership and operating strategies. Therefore this could apply to a company's cyber security strategy. We conducted a series of in-depth interviews and qualitative analysis with the goal of identifying key roles and influential drivers within companies; allowing for greater understanding of security related decision-making at board and senior management level.

5.2 Method

Ethical approval for this study was granted from the Northumbria University Psychology Ethics Committee. The study aims to investigate the identified gaps in the current knowledge using a dual-pronged approach:

1. Investigate and summarise wording of current insurance policies and business security policies; to identify whether these documents suggest who will be making cybersecurity decisions in companies, and whether cyberinsurance features in business security policies.

The insurance policies were collected via an internet search using the search "cyberinsurance OR cyberinsurance OR cyber-insurance, type: pdf". A similar search was conducted for organisational security policies ("security policy OR risk register, type: pdf") within companies.

2. Stakeholder interviews. Individual interviews with decision makers within businesses, and with individuals involved in the sale/marketing of cybersecurity products such as cyberinsurance; to identify hands-on experience and perspectives of cybersecurity policy and the decision-making process preceding purchase of cybersecurity products including insurance.

A total of 11 in-depth interviews were conducted with individuals responsible for making cybersecurity decisions within a company, and individuals involved in the marketing and/or sale of cybersecurity related products or services. We used an approach similar to that applied by Weishäupl *et al.* (2018) by interviewing a combination of companies, and also consulting partners such as insurance brokers. The rationale behind this is that companies may sometimes be reluctant to disclose security-related inadequacies due to concerns around potential attacks and/or damage to reputation (Turoff & Plotnick 2012). This provides us with data from those with first-hand knowledge of how decisions are made within their company, and also those who are experts in cybersecurity and work with various companies on a regular basis (and may be more willing to disclose potential vulnerabilities). The sample details are shown in Table 5.1.

Interviews lasted on average around 45 minutes and took place in person or via Skype. The interviews were transcribed and qualitatively analysed to identify the processes behind cybersecurity decision-making in companies. Analysis was conducted using NVivo, a specialist software for qualitative data.

The interviewees were asked about all elements of cybersecurity including implementation of security controls, purchase of cyberinsurance and staff training. One of the main discussion points during the interviews was around how cybersecurity decisions are made within the companies that they have experience with. The interviews were flexible and open to allow the conversation to progress naturally around the topic.

5.3 Results – Phase 1: Risk registers, insurance policies and business security policies

Wording of 12 different cyberinsurance insurance policies, and 20 organisation security policies/risk registers was collected. The policies were then analysed to identify whether they suggested who was responsible for cybersecurity issues.

Of the insurance policies, none specified who would be responsible for making the insurance decisions or taking out the policy. One policy defined the policy holder as:

> *"Any person who was, is or during the period of insurance becomes your partner, director, trustee, in-house counsel or senior manager in actual control of your operations"*

The wording in this policy also suggested someone responsible for the overall business, for example referring to "your business" and "your employees". However, outside of this none of the insurance policies, we identified online, specified necessary criteria for the policy holder.

Many of the insurance policies were vague in what they regarded as the minimum necessary security procedures to have in place. For example:

> *"All reasonable steps to prevent an insured event arising or continuing"*
>
> *"Backup systems"* and *"all things reasonably practicable to avoid or diminish any loss"*
>
> *"Back up data at least every 7 days and protect systems with a firewall"*

Looking across 9 business security policies and 14 risk registers there was a range of staff identified as responsible for cybersecurity: The director of IT/Head of Technology, COO, Deputy CEO, Financial Services Manager or FD, Emergency Planning Officer, Chief Technology Officer, CISO, CIO, Director of Strategy & Performance. Suggesting that there is not likely to be a universal member of staff responsible for cybersecurity decisions within companies. This is explored further in the following section during the interviews with stakeholders.

Of the 23 documents, all but two specifically mentioned cyber risk (the two in question referring only to IT system failure but no intentional and/or external cyber risk). However, **every security policy and risk register** failed to mention cyberinsurance. Security measures mentioned included:

- IT policies and staff training
- Incident reporting
- Access and network management
- Audits
- Secure media destruction
- Encryption
- E-mail scanning
- Data backup and recovery plans
- Business continuity plans

- Antivirus and anti-malware software
- Penetration tests
- Enforced password changes
- Regular patching & updates

This suggests that cyberinsurance is not yet recognised in many businesses as an integral part of cybersecurity.

5.4 Results – Phase 2: Stakeholders Interviews

Analysis of the stakeholder interviews identified 3key themes. Firstly that the company decision-making process is complex and involve multiple people and responsibility does not lie with a single person. This can make decision-making slow and prone to delays. Secondly, there appeared to be internal conflict surrounding the usefulness of cyberinsurance, with some opting for increased security rather than insurance or even not perceiving security as an issue. This conflict was fuelled by difficulties in measuring cyber-risk on which insurance is based, perceived immaturity of the cyberinsurance market and lack of trust in insurers. Lastly environmental changes in terms of new data protection legislation (GDPR) was perceived to be driving uptake of cyberinsurance.

5.4.1 Complexity of the company-level decision-making process

Many of the interviewees commented that decisions around cybersecurity are not made by one person but often involve a number of people within the business. For example, these decisions may involve the CISO, security board, COO, FDD, IT team, various committees and the executive board. This is particularly true for larger companies, with the decision-making process increasing in complexity with the company size.

> *"I doubt whether you'd get one single person, you might do, in a medium to smaller organisation [. . .] But I think you now get panels, like a risk committee and get someone from the security discipline, someone from the IT discipline, you get an auditor, you get compliance and those type of people. . . "*

> *"We have a security operations team, security engineers, security architects, government risk compliance team (for internal and external audits), security awareness staff, third party and supplier insurance, and a team that worries about email and end point security, a forensics team and an identity management team. The last team is a security platforms team that run a lot of the systems we run on. The team is about 140 people. [. . .] We also have a risk committee"*

This shows that within the role of the company (Figure 5.1), there is a whole ecosystem in itself. Because of the complexity of these systems and the number of parties involved, cybersecurity decisions at company level can be time-consuming and complex:

> *"It can take months, particularly in a complicated organisation with so many markets and people so in order to put something proactive in place it takes months of embedding. So it is a challenge"*

Although the final process of 'signing off' a security related purchase may be quick and efficient, unfortunately there can be significant delays reaching this stage. This can be due to time consuming processes involved in identifying and testing potential products:

"We'd go to procurement with details on what we have done, what we want, how much it is to buy. The CPO then signs it off based on my teams work. My team would probably have worked on this over a 6 month period (meeting about 6-10 times for an hour or so each) the meeting with the CPO then takes about 15 minutes.[. . .] It is always a much longer process than I've been willing to accept. [. . .]"

Interviewees also reported restricted periods when decisions can be made (e.g., dates of quarterly committee meetings, or annual windows for budget allocation), and further delays due to negotiating contracts with product providers and contractors:

"Even just another 3 months to get contracts into place. Getting contracts into place always involves a lot of negotiation and back and forth with the contractors"

When talking about cyberinsurance adoption specifically, interviewees often described a slightly different decision process – compared to other cybersecurity decisions. For example insurance adoption was often being driven by departments outside of the technology or cybersecurity departments, such as finance departments and risk committees. Interestingly, this often leads to a level of internal conflict around these decisions (discussed further in Section 2).

"I have only ever seen insurance requirements come from finance you know the FD is effectively responsible for insuring the business against risk. [. . .] I have never been in a position where the security person has gone to the finance person to say I think we need insurance"

Of course not all of our interviewees had cyberinsurance – for example, the smaller companies (SMEs) often reported not having a current cyberinsurance policy. This decision was often justified by statements about the business not being mature enough or big enough to merit cyberinsurance, or due to financial constraints within the company:

"At the end of the day if you're paying out so much premium you just take the risk."

"[If] the cost of the controls exceed the profit you're going to make and the cost of the insurance premium you know, you haven't got a business. I think a lot of people must arrive at that decision"

This suggests that adoption of cyberinsurance is likely to occur at a later stage in business maturity, rather than being something that businesses adopt from the start.

5.4.2 Internal conflict around cyberinsurance adoption

Interestingly, within the larger companies (who did tend to have cyberinsurance policies) the decision to adopt these policies was not always unanimous. As aforementioned (Section 5.4.1) the decision to adopt cyberinsurance was often driven by departments outside of the technology or cybersecurity departments. Many of the interviewees described a disconnect between the various influencers and decision-makers within the company. Some stated that they would not have personally opted for insurance, despite their company doing so. For example, one interviewee declared that as technical director, he would not have chosen to purchase cyberinsurance for his company, but that this decision came from outside of the cybersecurity team:

"We have a cyberinsurance policy at the moment. I must admit it wasn't me that made this decision. As I'm not sure I would have bought one, if I'm honest. The decision came from the risk committee. [. . .] It feels like it is boards outside of cybersecurity teams that make decisions to buy cyberinsurance."

Other interviewees described differences in priorities between committees, the board, and other staff involved in the decision-making process:

> *"The board owned the purse strings but it's interesting – they made the decisions because they owned the budget I suppose but they weren't very interested. [...] We [the IT team] would be setting out the risks and the threats trying to explain to them why they need to spend more and there would be certain threats they would get very excited about and others that maybe they would be less interested"*

> *"They [the board] weren't particularly worried about passwords. They were a bit concerned by phishing because obviously they could be – but I don't think they were that interested in that to be honest, I think they expected us to be creating a basic level of security the things they got excited about was if something came to bail on them or they would become personally liable"*

We investigated the factors why there may be this disconnect between decision-makers within companies when it comes to cyberinsurance. Three key themes were identified: a) *security versus insurance*, b) *immaturity of cyberinsurance and lack of data on cyber risk*, and c) *mistrust of insurers*. These are discussed in more detail in the following sections.

5.4.2.1 Security vs. insurance

For some of the interviewees, security measures were perceived as being more important than insurance policies. With some individuals perceiving insurance as not being required, if good security measures were in place:

> *"I suppose when you're actually putting controls in, there is a form of insurance. So all you are really doing is, do you pay out some more money for some other controls which you understand or do you transfer that risk out? [...] I suppose the counter argument is the individual risk is, and you put additional controls and pay for it that way"*

Perceived vulnerability also appears to play a role, with those who perceived themselves as knowledgeable [with IT/cybersecurity] reporting that they would be unlikely to take out cyberinsurance. Therefore perceptions of self-efficacy around cybersecurity appear to influence decision-making around cyberinsurance. Suggesting that greater awareness of cybersecurity may not necessarily lead to greater uptake of cyberinsurance. Instead perceived self-efficacy could lead to a false belief that insurance is not necessary (due to being able to protect themselves).

5.4.2.2 Immaturity of cyberinsurance and lack of data on cyber risk

The reluctance to invest in cyberinsurance may also be linked to concerns around the immaturity of the cyberinsurance market, and lack of awareness about what is covered by cyberinsurance policies. Interviewees also commented upon a perceived 'grey area' between what is covered on traditional insurance and what is covered by cyberinsurance. This uncertainty may help to explain why there is a reluctance to adopt insurance policies, and/or why businesses would rather spend their money on more tangible security measures which they feel personally in control of, and/or feel they understand more:

"That [security] control could last all you wanted to or you could change that control as it's under your direct management"

The lack of data on cyber risk also makes it difficult for businesses to be able to measure and quantify their own risk:

"The threats are difficult to measure. [. . .] generally speaking the data is not available in organisations to make accurate decisions"

"I have had conversations with the marketing people around what happens if we suffer a cyberattack and. . . those were interesting and not conclusive they basically said we have no idea we have never had one. We can't get data from people who have had one"

A general lack of awareness around cyber risk was articulated, across all organisations and insurers. However, the insurance brokers and consultants that we interviewed perceived this as being a particularly strong concern for smaller businesses – who they did not perceive as being able to accurately assess their cyber risk. Despite these difficulties in quantifying risk, companies are asked to do exactly that when they try to take out an insurance policy, i.e., in order to answer the various questions posed to them by insurers. This can lead to anxiety on behalf of the businesses and concerns whether the insurance they are putting in place is adequate and appropriate:

"The questions they ask on the policy form it was difficult to quantify the impact of that, it could have been three million it could have been fifty million... So it's an interesting one, yeah that was a risk to me"

Risk assessments were perceived as undoubtedly difficult – however interviewees suggested that they could potentially be made slightly easier by focusing on how risk is measured. For example, by asking about risk in less technical terms. This was raised as particularly relevant for SMEs:

"I don't think they [SMEs] would understand the technical risks, I think they would understand if you spoke about what assets you have got – I think if you spoke to people about trying to do a business continuity plan then saying what applications do you need back up – it's always quite hard to have that conversation with them [. . .] If you structure the questions right you can [ask]. . . what are the systems you absolutely need – what is the biggest risk"

"So I think that is the thing for SME's is how can they quantify the impact it's going to have on their business, I would use impact assessments rather than just risk assessments because it is far easier. What happens if you don't open your shop today – you know your shop could be online, well that's easy I lose business, how much business do you lose each day? You know, you can do that quite easily. But if you say what is the risk of your website going down, that is really hard to quantify"

5.4.2.3 Mistrust of insurers

Some interviewees expressed negative views of insurance companies including doubts around the intention of insurers and the likelihood of paying out. Interviewees perceived insurers as using complicated policy wording and exclusions to their advantage, i.e., to find a way to not pay claims:

"One of the key reasons I am not an advocate of insurance policies is there is always a way of not paying out"

"I feel like – anybody that I talk to in the cybersecurity industry feels that cyberinsurance is a joke and that it never pays out"

Interestingly, one interviewee explained how they perceive media coverage as reinforcing negative views of cyberinsurance:

"It gets a lot of media attention. For example, the chocolate company that are suing their cyberinsurance company that won't pay out over NotPetya as they're classifying it as an act of war. When its reported in the type of stuff that the industry looks at.. because we're all already quite cynical about cyberinsurance.. the reporting comes across biased, quite cynical. It's like 'we all knew it was true and look now it's happening [the insurance aren't paying out]"

This suggests that media coverage around cybersecurity could be a double edged sword. For example, it may not only have the potential benefit of increasing awareness around cyber-risk (although admittedly these may be biased by recent events) but it may also reinforce negative perceptions of cyberinsurance.

5.4.3 Compliance Legislation as a driver for cyberinsurance adoption

External influences on cybersecurity decisions were reflected in the interviews. For example one interviewee recalls being shocked when the COO of a cybersecurity company was only concerned with being as secure as their competitors! Another external driving factor emerged in the majority of the interviews – compliance with legislation. This is in keeping with findings from Heidt *et al.* (2019), Weishäupl *et al.* (2018) and Chew *et al.* (2008) who argued that investment in information security is largely driven by external environmental and industry-related factors, including legal regulations and industry-specific demands and requirements. One of the insurance brokers we interviewed described an increase in insurance uptake following the introduction of the GDPR. This echoes recent findings by Heidt *et al.* (2019) who found that the GDPR not only influenced decision-making at the basic level of whether to invest or not, but also what areas to invest in and the level of investment. This could be due to the introduction of legislation helping to quantify risk, e.g., if there is a data leak you will be fined a considerable amount of money. Interestingly the interviewee in our study also commented that the effect of the GDPR on cyberinsurance purchasing was already showing signs of decreasing. This suggests that cyberinsurance (and cybersecurity more generally) may be affected by recency effects, e.g., risk being perceived as higher for threats recently mentioned by policy and/or media events.

Despite this, there were some concerns that insurance is not always providing adequate coverage in some situations. For example, one interviewee doubted whether many insurance policies would be enough to adequately cover the damages caused in the event of a cyberattack and instead described purchasing insurance as a means to "look as if you are covered". Another interviewee reflected on a time when their company discovered they did not have adequate insurance in place to cover their online database of around £500 million electronic shopping vouchers:

"Because it is a cash equivalent it is not covered under the cyberinsurance policy. So you turn to our insurable risk team and ask how much is covered on our crime policy

and find the maximum payout is £5m. So they had to run off and find the crime policy has never been right and should have always been higher than that"

This also relates back to the aforementioned confusion around the 'grey area' between traditional and cyberinsurance (Section 5.4.2).

5.5 Conclusion

The findings highlight that the decision-making process at company level involves a complex ecosystem in its own right. These systems can vary dramatically between companies, depending upon size, maturity and sector. There is not a universal 'one size fits all' cybersecurity structure within companies. There are also many different factors, both internal and external to the company, that can influence cybersecurity decision-making and cyberinsurance adoption. Any cybersecurity services, interventions and/or products need to account for this variation within the decision-making process.

Different cybersecurity-related decisions may be driven by different departments, teams and/or factors. For example, cyberinsurance adoption often seems to be driven from outside of the technical teams (for example from finance) and appears to be largely influenced by policy and legislation. In keeping with recent research by Weishäupl *et al.* (2018) our findings suggest that there may be a disconnect between the academic literature that sometimes regards security decision-making as intrinsically motivated, and the emerging literature (such as the current study) that shows that companies may be more motivated to invest in security because they need to in order to comply with legislation. Legislation as a driver for cyberinsurance also fits within the Burke and Litwin model (Figure 5.2). As previously mentioned, this model suggests that the most dominant factor on organisational performance and change is the external environment. External environment could include factors such as those mentioned in our interviews, e.g., recent media coverage of cyber-risk and governmental legislation such as the GDPR. In much the same way as Burke and Litwin, we show that in relation to cybersecurity decision-making in companies, external factors appear to have a strong influence. However, internally to the company there are many different processes also influencing these decisions – including a complex (and non-universal) company structure across many different boards, committees, teams and departments. Each reflecting their own motivations, priorities, and processes. Priorities and perceived threats may also differ between staff members, boards, committees and departments.

In keeping with Weishäupl *et al.* (2018), we found evidence that companies can perceive security-related decision-making (and related processes) to be timeconsuming and effortful. For example, even the process of acquiring an insurance quote (and gathering the associated company information needed to obtain this) and the renewal process were seen as effortful. The has the potential to have a detrimental impact upon cyberinsurance adoption, and is further compounded by lack of awareness around cyber risk, cyberinsurance coverage and a mistrust of insurers in regards to transparency of coverage and uncertainty around payout in the occurance of a cyber breach. Resource and financial constraints also play a role.

Many approaches to cybersecurity still assume a rational decision-making process. However, cybersecurity decision-making cannot be accounted for by purely rationalised processes and accurate calculations of benefit and risk. The accurate calculation of risk is unlikely at best, currently due to a lack of data on cyber risk and how to measure it and the benefits are under debate.

7.1: CYBECO Policy Recommendations

In relation to policy recommendations, our findings suggest that businesses may appreciate more detailed cyberinsurance policy wording regarding the specific terms and conditions of coverage (e.g., inclusions and exclusions). However as identified in Section 4.4 (in relation to legislation), specificity can make it difficult for policies to take into account the changing nature of the cybersecurity environment. Therefore a balance is required between providing enough detail to reassure and/or guide companies, whilst maintaining enough room for the policies to take into account new developments in cybersecurity risk and protection. Further research is required to investigate the most appropriate level of specificity. Legislation or standardisation of cyberinsurance policy wording could help to reassure companies, and also address confusion over what is covered by the policies (and clarify the perceived 'grey area' between traditional insurance policies and cyber policies).

Companies also expressed mistrust in insurers, therefore policy makers would benefit from a better understanding of best practices that could help build trust between the insurer and the insured. Information sharing is key to achieving greater awareness around cyber risk and improving practice, but the absence of good cyber incident data is problematic here (see Section 5.4.2). Policy measures to increase anonymised data sharing would be beneficial in this regard. However, appropriate methods to implement of this require further investigation.

Lastly, within companies, the organisational infrastructure around cybersecurity decision-making varies widely – with many different actors involved in the company ecosystem (see Section 5.4.1) and a degree of confusion and sometimes disagreement between the different parties. Understanding more around the organisational structures and the various roles and responsibilities for cybersecurity and cyberinsurance decision-making would be beneficial.

6 Cyberinsurance adoption among Dutch SMEs: a qualitative study

Protective measures like security awareness, intrusion detection systems, and a safeguarding infrastructure, among others, may limit the risk of cyber attacks. However, security measures alone may be insufficient due to the regular development of new attack modes, malware or increased attack sofistication. Since it is not possible to fully protect the company's systems, an appropriate combination of risk management strategies is of great importance for any company using information technologies (IT). There are five main strategies of risk mitigation: 1) accept, 2) avoid, 3) mitigate, 4) share and 5) transfer (Stoneburner *et al.* 2002). Cyberinsurance is related to the cyber security risk transfer strategy. Besides transferring financial exposure, cyberinsurance is also contributing to the cyber risk management by raising awareness, supervising incident management and encouraging investment in security systems. While the promise of cyberinsurance is high, adoption rates have fallen short of expectations regarding market uptake, 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 (CIAB May 2017), and the U.S. is the most developed market by having 90% of the global cyberinsurance market, while Europe counts for just 9% (OECD 2017b).

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 (Kuypers *et al.* 2016, Romanosky 2016). Finding these limitations in the existing academic research raised questions about the validity of this knowledge for small and medium-sized enterprises (SMEs) and countries that have not seen many attacks.

If parallel lines are drawn between acquiring cyberinsurance and getting any other type of insurance, previous research has shown that under risk conditions humans do not behave rationally Briggs *et al.* (2018b). Then, if this is also true for cyberinsurance adoption, a different approach to understanding the reasons for the low rate among SMEs on getting cyberinsurance could be considered relevant. The traditional method for this has followed the use of quantitative and mathematical models of the cyberinsurance market (e.g., (Hayel & Zhu 2015, Tosh *et al.* 2017, Yang & Lui 2014), but these models lack realistic behavior of decision-makers regarding cyberinsurance. One way to look at this problem is by analyzing how individuals make decisions when purchasing cyberinsurance in the condition of a lack of detailed information about company's risks. In light of the size of the study, the scope of the research has been set at SMEs in the Netherlands. Therefore, we formulate the main research question as follows: *What mechanisms and factors explain how Dutch SMEs decide on cyberinsurance adoption?*

To address this question, we applied the Protection Motivation Theory (PMT - as also applied during the CYBECO economic experiments Briggs *et al.* (2018b)) which is a behavioral theory that identifies the elements guiding a decision maker to determine whether to protect against a threat or not. We used PMT as an underlying theory to explain the reasons why SMEs decide to select protection against cyber risks. This study focused on the following PMT elements: intrapersonal and environmental sources of information, vulnerability, severity, rewards, response efficacy, self-efficacy and response costs, to find the reasons why companies adopt (or do not adopt) cyberinsurance. The full report on this study is available in (Martinez Bustamante 2018).

6.1 Protection Motivation Theory for cyberinsurance

In this section, we adopt the definitions of PMT from Floyd *et al.* (2000) and illustrate them with examples from the cyberinsurance domain to allow PMT application to the cyberinsurance context. See CYBECO D6.1 deliverable for the details about PMT (Briggs *et al.* 2018a).

1) Sources of information contain the arguments regarding potential victimization threats, potential protective options, and reasons why the decision maker would conclude that one should or should not engage in getting cyberinsurance. It consists of the following elements:

- ***Environmental sources***: *verbal persuasion* like discussion with colleagues, clients or other companies about cyberinsurance; *observational learning* like knowing a company that has suffered a cyber attack (beyond what the news reports), or a company adopting cyberinsurance after directly witnessing a cyber attack.
- ***Intrapersonal sources***: *personality aspects* like the professional background, role in the company and knowledge about cyber security; feedback from a *prior experience* like directly witnessing a cyber-attack.

2) Threat appraisal evaluates an undesired behavior is composed of the next elements:

- ***Vulnerability***: a subjective assessment based on information about the company that it will experience harm. Example: if a company believes it is susceptible to a cyber attack, maybe because the company's business is of interest of attackers or because they have taken precautionary measures with its IT security.
- ***Threat severity***: an assessment by the decision maker of the degree of harm from an attack based on information available to them about the company. Example: if a decision maker thinks that the company is susceptible to attacks, it is necessary to know the attacks they are more afraid of and their perception of the attacks severity.
- ***Rewards***: *extrinsic rewards* like avoid expenses which are perceived as unnecessary or the absence of sanctions for not having a cyberinsurance; *intrinsic rewards* can be the beliefs that a measure is not useful because (1) the likelihood of cyber attacks is low, (2) it is not included in the company security guidelines, or (3)there is a perception that the company is capable of protecting by itself.

3) Coping appraisal enables the decision maker to evaluate the ability to avert danger and if necessary cope with it. It includes the following elements:

- ***Response efficacy***: an assessment by the decision maker of the relative effectiveness of the chosen response, e.g., having cyberinsurance.
- ***Self-efficacy***: the perceived ability of the decision maker to carry out the chosen responses, e.g., how much the person knows about the cases when the cyberinsurance can be used or how able the company has been by dealing with a cyber-attack.
- ***Response costs***: any costs associated with getting cyberinsurance: premiums, deductibles, cost of implementation of cyberinsurance policy requirements. There could be an adverse effect of having cyberinsurance like moral hazard leading to lowering the level of security because the company knows that in case of an incident cyberinsurance will cover it.

6.2 Research method and study execution

The goal of our study is to investigate which of these PMT factors affect cyberinsurance adoption among Dutch SMEs. Similar to the study reported in chapter 5, we choose a qualitative approach consisting of a series of semi-structured interviews with SMEs' representatives which is a suitable method for our research problem. The PMT concepts discussed in the previous section served us as a framework for formulating a semi-structured questionnaire to guide our interviews with SMEs' representatives. See Table 6.1 for the semi-structured interview guide.

6.2.1 Data collection

We worked with an insurance broker to reach SMEs for our study because brokers can represent several insurance companies and their knowledge of organizations with interest in cyberinsurance seemed like a natural place to start. We tried an alternative way to reach SMEs via the sectoral organizations as they represent the companies' interests of a specific sector. However, we got zero response throughout this channel.

The broker provided us with the contact details of 17 companies, but only 10 of them agreed to participate in our study. All participants received a consent form in advance of the interview which explained the research objectives for which the data would be used and guaranteed the anonymity of the interviewee. The interviews were conducted between May and July 2018. Table 6.2 summarizes the interviewees by sector, SME type, security management situation, scenario, the lifespan of the cyberinsurance (if the company already has one) and if IT services are outsourced or not.

6.2.2 Data analysis

The interviews were recorded and transcribed for textual format for further analysis. The first step of the analysis is open coding where non-structured codes are created, meaning that no code is assigned to a "higher range" code, avoiding tree structures. The open coding identifies text segments, as these segments can have one or more codes assigned and each code interprets that statement in a brief word or group of words. For example, the statement *(1) "I know that you can insure for anything you would like, but I wasn't aware there was this specific insurance. (2) I also thought it was part of the liability insurance but then I was approached, and the broker said it wasn't the case, that I needed a special product."* we marked with the following codes: *PMT: Sources of Information (Intrapersonal)* and *Information Sources – Knowledge by insurer or broker*; for (2) we also assigned code *Cyber Insurance Impediments – Silent coverage*.

After the open coding was done for all the interviews, group codes were created based on relevant themes related to the factors asked in the interview questions (see Table 6.1). Example of these themes is companies' experience with cyber attacks, cyber security knowledge, cyberinsurance knowledge, security threats, opinion about the business process, security controls in place, insurance policy, and other. Notions with similar meaning and a low number of statements were grouped into one code. In total, we extracted and coded 517 different statements in 10 interviews. Table 6.3 reports the number of statements by interviews and categories like PMT elements, drivers and impediments.

Table 6.1: Questionnaire for SMEs per scenario (Martinez Bustamante 2018)

The semi-structured interview questionnaire per scenario grouped by PMT elements. PMT components do not have explicit questions as they are defined by the corresponding elements.

PMT concept	1. Has CI	2. Is considering CI	3. Does not have CI
Sources of information	**No question**		
Intrapersonal	1) Is your role in the company related to keeping the company secure from cyber threats? 2) How did you first hear about cyberinsurance? 3) Do you know companies who already have a cyberinsurance?		
Environmental	1) Have you discussed the cyberinsurance topic with your clients or other companies? 2) If yes, what was their opinion about cyberinsurance? 3) 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 cyberinsurance?		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 cyberinsurance?	What are the main security threats for which you would get a cyberinsurance?	What are the main security threats you consider relevant to the company?
	Do you think some of them have more impact than others?		
Rewards	1) Is any of the next reasons a potential cause for you to not select a cyberinsurance? - Do not get a cyberinsurance until other companies do so. - There are no sanctions for not having a cyberinsurance. - Do not buy cyberinsurance to save budget. - It is not included in the security guidelines of the company. 2) 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 cyberinsurance policy?	What expectations do you have if you decide to get a cyberinsurance?	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 cyberinsurance and in which cases you would be able to use it?	Do you fully understand the coverage *offered* by your cyberinsurance 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 cyberinsurance?
Response cost	What potential drawbacks would you associate with adopting a cyberinsurance?		No question related
	What do you think about the premium price?		

Table 6.2: Demographics of interviewed SMEs (Martinez Bustamante 2018)

ID	Sector	SME type[1]	Someone in charge for security management?	Scenario	Lifespan of CI [months]	External IT/security provider?
I01	Legal services	Small	No	1	18	Yes
I02	Wholesale	Medium	No	1	18	Yes
I03	Financial	Medium	Yes, partially	1	4	Yes
I04	Financial	Micro	Yes	3	NA	No
I05	Financial	Medium	No	2	NA	Yes
I06	IT	Small	Yes	1	30	No
I07	Installation	Small	No	1	12	Yes
I08	IT	Small	Yes	3	NA	No
I09	IT	Medium	Yes	3	NA	Yes
I10	IT	Medium	Yes	3	NA	Yes

[1] SME size: Micro: 1 - 9 staff headcount; Small: 10 - 49 staff headcount; Medium: 50 - 249 staff headcount (European Commission n.d.).

Table 6.3: Number of codes per PMT elements, drivers and impediments

Category/ Element	I01	I02	I03	I04	I05	I06	I07	I08	I09	I10	Quotations
Threat appraisal	13	10	20	20	18	24	11	21	17	9	163
Vulnerability	9	5	19	14	11	16	7	13	11	3	108
Rewards	3	4	0	2	5	4	3	3	2	5	31
Severity	1	1	1	4	2	4	1	5	4	1	24
Coping appraisal	10	12	13	10	11	12	7	4	5	7	91
Self-efficacy	3	7	6	7	2	3	2	2	1	2	35
Response efficacy	5	1	3	2	5	6	3	2	3	4	34
Response cost	2	4	4	1	4	3	2	0	1	1	22
Sources of information	6	5	11	3	7	11	5	3	4	4	59
Environmental	3	2	5	3	4	8	2	1	2	0	30
Intrapersonal	3	3	6	0	3	3	3	2	2	4	29
Drivers	8	8	7	1	9	5	4	1	4	1	48
Impediments	1	1	0	3	6	1	0	4	2	0	18

6.3 Results

We report our findings by PMT components and elements expanding each category with factors specific for cyberinsurance adoption. We also discuss possible drivers and impediments affecting the decision-making process of SME's representatives. At the end of the section, we summarize these findings into a conceptual model of cyberinsurance adoption.

6.3.1 Sources of information

Sources of information is the only PMT component for which the same questions were made to all the companies regardless of the scenario they related to. Table 6.4 shows the major factors that were identified for each PMT elements within the *sources of information* component. We report the co-occurrence coefficients (Contreras 2011) between codes and PMT elements to show the strength of relations between them.

The ***intrapersonal*** element deals with personality aspects and feedback from prior experience, which is, how did the company's representative first heard about cyberinsurance. Four

Table 6.4: Co-occurrence of codes and PMT elements related to the source of information component

Environmental	Intrapersonal
External experience (28%)	Responsible for security/safety/insurance (19)%
Cyber security incident (24%)	Knowledge (by insurer/broker) (18)%
External sources of information (18%)	Cyber security knowledge (7%)
Cyber attacks in the media (18%)	Security goal: Awareness (6%)
External discussion (13%)	

Table 6.5: Co-occurrence of codes and PMT elements related to the threat appraisal component

Vulnerability	Severity	Rewards
Alternative protective measures (22%)	Threat: Data leakage (10%)	Premiums price (17%)
Attacker motivation (12%)	Small company type (6%)	Cyberinsurance adoption: it is not necessary (15%)
Vulnerability: Digital communication (10%)	Threat: Phishing (7%)	Cyberinsurance adoption: No added value (10%)
Vulnerability: Cloud technology (10%)	Threat: Data loss (8%)	
Asset: Company's reputation (9%)		

representatives indicated they knew that cyberinsurance exists and three out of them were from the companies who decided not to get cyberinsurance. Two of these answers were about finding of cyberinsurance 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)***. Whereas the other two interviewees discovered cyberinsurance as a solution due to 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".* ***(I08)***. The rest of the companies' representatives heard about cyberinsurance for the first time from the broker.

The ***environmental*** element identifies the decision maker's external experiences like knowing about other companies that suffered a cyber attack and discussing with other companies about cyberinsurance, that would help him to identify threats and protective measures. Similarly, Section 5.5 points out that external factors have a strong effect on cyber security decision-making in companies. These external factors could cover, for example, *"recent media coverage of cyber-risk and governmental legislation such as the GDPR."*

6.3.2 Threat appraisal

Table 6.5 present the most cited codes related to the elements of threat appraisal component and the coefficient co-occurrence between codes and a corresponding PMT element.

The ***vulnerability*** element analyses the main reasons for decision makers to perceive a degree of probability that their companies could experience a cyber attack. The most cited category is the use of *alternative protective measures* as we discussed with interviewees what security controls their companies use in addition to cyberinsurance or in general. For example, *"[. . .] we now decided to start working with a client portal so we don't send emails with the documents to the clients [. . .]" (I01)*. The second category is an *attacker motivation* to attack a company: *"When people think there is money involved, could be a reason." (I02)*. At the same time, increasing *digitalization* and use of *cloud technologies* can make companies more vulnerable: *"We have our data in the cloud, so that makes us much more vulnerable. Although*

our IT company says it is better protected than the paper trail, I don't know, but that makes us more vulnerable" (I01). Another factor commonly mentioned is company's *reputation* because SMEs highly value their reputation: *"Because our reputation is all we have, we can't afford to be blackmailed [. . .]" (I03)*. They believe attacks can target this aspect, but they also believe reputation is something that needs to be protected.

Even if companies have cyberinsurance, we ask them whether they have other types of cyber risk security controls. In most of the cases, we had to make examples of possible controls, e.g., antivirus, firewall, and others. Overall, the most mentioned answers besides *firewall* (5 statements) were *security training* (5 statements), *identity and access management* (4 statements) to company's data and the implementation of *business contingency plan* (3 statements).

The next threat appraisal element is ***severity*** where we tried to find out if companies know how they could be attacked and the consequences of it. The most mentioned threats were *data leakage*, *phishing*, and *data loss*. Also, the *small size of the company* was mentioned in the context of lower threat severity: *"I don't think that anyone understanding the company's activities would target it as a high-value target" (I09)*.

Finally, the ***rewards*** element which indicates why the decision maker finds it attractive not to adopt cyberinsurance. The three main reasons that companies mention in this regard are *price*, that cyberinsurance is *not necessary* or brings *no added value*. These findings also support the results regarding decision-making strategies in Briggs *et al.* (2018a, Section 2.1.). Below we provide some statements to illustrate or motivate their reason:

> **Price:** *"If it cost too much we wouldn't have get it "* (I07).
>
> **Not necessary:** *"Another reason we didn't think it was really necessary"* (I01).
>
> **No added value:** *"[. . .] by putting the same amount of effort in technical measures we cover it better than doing it with the insurance"* (I09).

6.3.3 Coping appraisal

Table 6.6 presents the codes that the most frequently occurred together with the coping appraisal elements. After the threat is identified, the company looks for possible ways to mitigate it. For ***response efficacy*** element, if the company is in Scenario 1 the researcher asked if the insurer required to implement additional security controls to be insured. Whereas if the company is in Scenario 3, 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 1 and 2, question about their expectations towards the cyberinsurance would help to identify if by adopting this measure they felt able to deal with the risks.

Five companies made twelve statements about their expectations for cyberinsurance which we grouped in the following four codes:

- getting coverage in case of a security incident: (*"if you buy an insurance you want it to cover everything" (I08)*.
- getting an appropriate help during the process in case of an attack: *"If something happens, I hope the broker or the insurance company do what they promise" (I02)*.
- expecting not to use the insurance: *"My expectations are that we will never have to use it" (I06)*.
- having a 24/7 incident response management: *"They will take away the sorrow from us" (I05)*.

Table 6.6: Co-occurrence of codes and PMT elements related to the coping appraisal component

Response efficacy	Self-efficacy	Response cost
Cyberinsurance expectations (33%)	Policy: Clear coverage (13%)	Premiums: Price (43%)
Policy: Additional requirements (13%)	No cyber incident experience (11%)	Premium: Fair (30%)
Policy: Damage coverage (11%)	Additional services: Incident response management (9%)	Premium: Low (8%)
Additional services: Incident response management (10%)	Security controls: Security management strategy (5%)	Premium: High (4%)

Most of the companies mentioned no *experience with cyber incidents*: *"I'm not aware of any security breaches that have happened in the history of this company, so the measures that are in place seems to be in good balance" (I09)*. Three companies reported that there was a security incident in the company.

Regarding additional requirements, the companies said that the insurer asked *"just the normal rules, like fulfill the GDPR. Nothing extra" (I07)*. One mentioned that *" I use their requirements and advice to bring awareness to the company because they also gave advice on how to implement security measures." (I03)*.

The ***self-efficacy*** element analysis is split depending on the scenario. In case of Scenario 1, the self-efficacy is related to how a decision maker assesses company's capability to use the cyberinsurance, namely how well they understand the policy, its coverage, and the cases when the policy is applicable. The companies in this scenario indicated that: *" it was pretty straightforward and easy to understand" (I06)*. In Scenario 3, the self-efficacy element was assessed based on companies current IT security management plan. Typical statements about it were *"we are focused on what could have the highest impact on us" (I04)* or *"we feel that [they have a good security management plan]" (I03)*.

The last element, ***response cost*** is related to the premium price. Since the literature indicates that cyberinsurance prices are high, it could be a reason for companies not to get one. Our observations did not confirm this hypothesis. The interviewees opinions are distributed as follows: cheap price – 2 out of 10 companies: *"The cost is very low for the insurance" (I07)*; fair – 3 out of 10 companies: *"it's fair; otherwise we wouldn't have taken it" (I06)*; high, but goes down – 1 out of 10 companies: *"The premium price it's high, but it has been going down" (I02)*, and 4 out of 10 companies did not have an opinion about the price.

6.3.4 Drivers and impediments

In addition to the contribution of PMT elements into the decision-making process, we also looked for the primary drivers and impediments for getting cyberinsurance. Among the main drivers for getting cyberinsurance we identified the next factors:

- *Reputation.* It is the main asset that companies seek to protect through different risk mitigation strategies.
- *Sectorial regulator recommendations.* Some recommendations regarding strategies are coming from sectorial regulators. *"The fact that the local bar highly recommended, that was a very important reason to get the cyberinsurance" (I01)*.
- *Additional services.* The fact that cyberinsurance provides additional services motivates companies to get it: *"That was the unique selling point of the product, to have that person*

Table 6.7: Co-occurrence of drivers, impediments and codes

Drivers	Impediments
Company's reputation (11%)	Low risk probability (10%)
Sectorial regulator recommendations (6%)	Policy coverage (8%)
Additional services: Incident response management (6%)	Cyberinsurance process (7%)
Cyber security incident (5%)	Risk transfer via supply chain (7%)
Security awareness (4%)	Premium: High price (5%)
Small company type (3%)	Alternative protective measures (3%)

with experience, 24/7 available, that can coordinate the process, who will guide us" (I05).

- *Security awareness.* The increasing awareness and experience with cyber security incidents drive decision makers towards cyberinsurance adoption: *"Since last year they [national regulator] mentioned cyberinsurance. That was for us the reason to become more convinced that it was necessary to have such insurance and we also had one leaked of data" (I01)*. Chapter 5 also suggests that improving awareness around cyber risk could have a positive impact upon cyberinsurance adoption.
- *Small company type.* The last driver in favor of cyberinsurance that we found was the small company status: *"We are very small, but the risk is big. If something happens to a small company, we could be closed" (I08)*.

The ***impediments*** are mainly gathered from the problems detected by the companies during the process of acquiring cyberinsurance. We identified the following key impediments for cyberinsurance adoption:

- *High price.* It was one of the reasons for not getting cyberinsurance: *"When the broker started with the offer the premium was much more higher than it is now, at that point that was one of the reasons to not get cyberinsurance" (I01)*.
- *Low risk probability.* It is another reason for not getting cyberinsurance as *" [. . . risk] almost doesn't occur. The impact is huge, but the chance is unlikely" (I08)*.
- *Policy coverage.* The doubts in *policy coverage* might block the decision about getting cyberinsurance: *"I have low confidence that a claim would be successful" (I09)*. This finding supports the conclusion made in Section 5.5 that cyberinsurance adoption can be improved by mitigating a lack of awareness around cyberinsurance coverage.
- *Cyberinsurance process.* A complicated *cyberinsurance process* might make cyber insurance adoption more difficult: *"The problem is you have to fill out a lot of forms to get the insurance" (I02)*. A similar observation was main in the study reported in Chapter 5 where companies perceived security-related decision-making as a timeconsuming and effortful process.
- *Alternative protective measures.* This reason was mostly mentioned by IT companies who believe that they have enough implemented security measures: *"We have to implement all the measures to have a secure platform" (I08)*.
- *Risk transfer via supply chain.* One of the interviewees believed that *it's not necessary for us to have insurance because [service provider] is taken care of [risk] (I04)* and, therefore, they *transferred risk* to their supplier.

6.3.5 A Model of Cyber Insurance Adoption among SMEs

Based on the findings of our data analysis presented above we built a conceptual model which describes what aspects affect decision makers to adopt cyberinsurance among SMEs (see Figure 6.1).

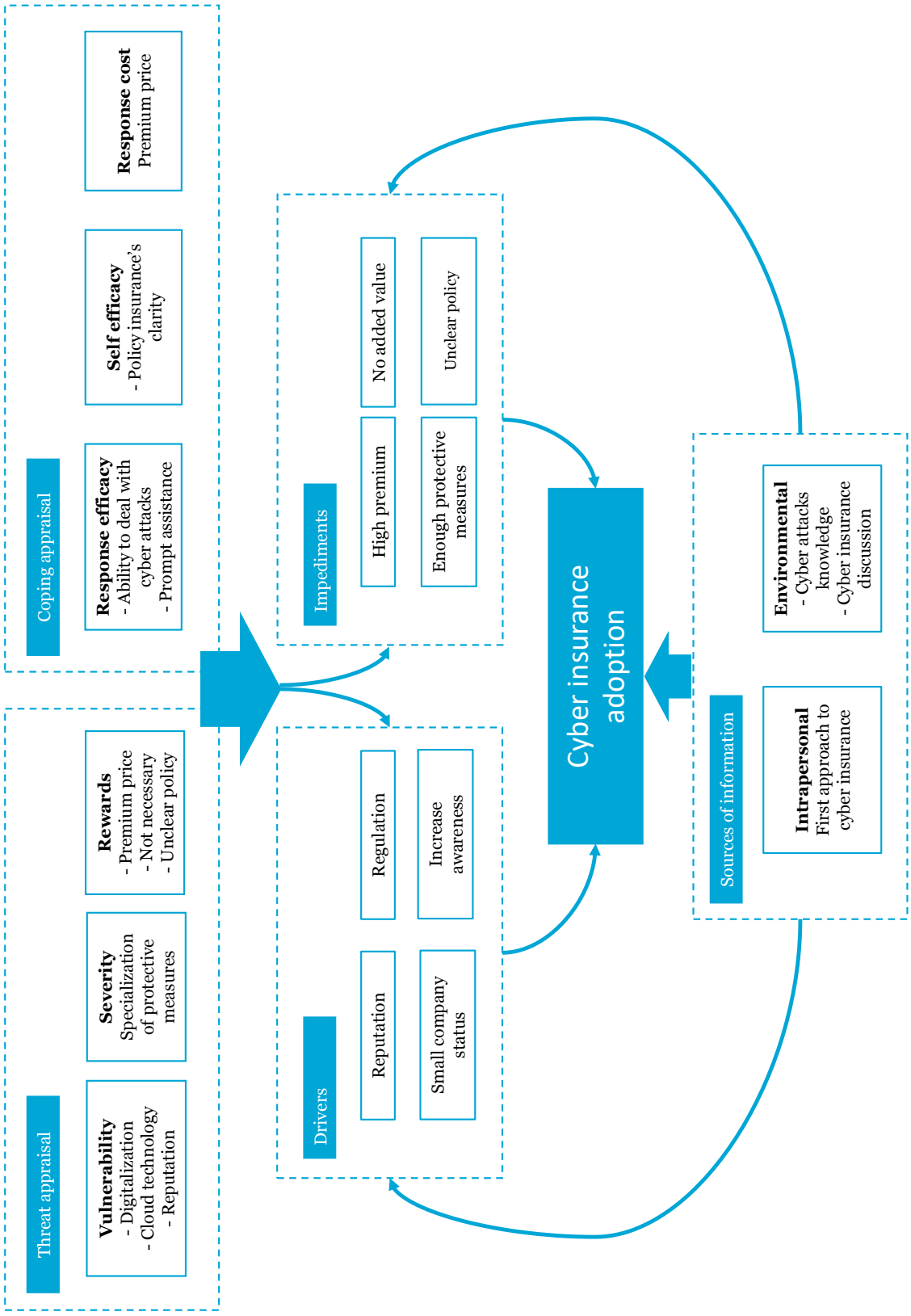

Figure 6.1: Cyberinsurance adoption model (Martinez Bustamante 2018)

The decision to adopt cyberinsurance is the central part of our model. The remaining components describe the cognitive process that SMEs representatives follow when making decisions regarding buying cyberinsurance. Overall, our model extends PMT with the factors identified in the interviews with decision makers and specific to cyberinsurance domain. The threat and coping appraisals are translated into a set of drivers and impediments for the decision-making process for cyberinsurance adoption.

A similar cyberinsurance adoption model is proposed within the CYBECO project by Briggs *et al.* (2019). In this case, a Structural Equation Modelling (SEM) is estimated from the experimental data of 4,800 participants of an online behavioural-economic experiment run in Germany, Poland, Spain and the UK in June 2018.

During the experiment, participants were asked to imagine that they were security managers of a small business. They were then asked to complete an online task (registering for a conference) and informed that they may suffer a cyber attack whilst completing this task. Participants were provided with an initial indemnity at the start of the task. Before registering for the conference, participants were offered the chance to opt for Advanced Security Measures (ASMs) to reduce the probability of suffering the attack and to Premium Insurance which payback part of the potential losses generated by a cyber attack. At the end of the experiment, participants received a payout dependent upon their decisions during the experiment and whether, or not, they suffered a cyber attack.

The model for cyberinsurance adoption is shown in Figure 6.2. This model shows a strong, significant positive pathway between the adoption of security measures and the adoption of Premium Insurance. This is the strongest pathway in the model. Security measures adoption is also significantly positively related to the security of online behaviour (the pathway between insurance adoption and online behaviour although positive fails to reach significance once the adoption of security measures is introduced into the model). Response efficacy and the factors of Theory of Planned Behavior (like intention and attitudes) are still positively related to the adoption of Premium Insurance, whilst perceived self-efficacy and perceived threat severity both positively feed into the adoption of security measures (which as aforementioned subsequently feeds into premium insurance adoption). Risk propensity is negatively related to both the adoption of security measures and insurance adoption (see “Dospert” variable in Fig. 6.2).

6.4 Conclusions and discussion

The main contribution of this study to the policy framework is providing a better understanding of the mechanisms and factors explaining how Dutch SMEs decide on cyberinsurance adoption. Such decision-making process is complicated for an SME due to the lack of detailed information about company’s risks and dynamic nature of cyber risk. Our conceptual model extends existing PMT model with the factors specific to the cyberinsurance selection process and identified what the key drivers and impediments that decision makers face in this process are.

6.4.1 Component: Source of Information

For this component, we found that cyberinsurance is a new concept among SMEs which requires brokers and insurance companies to take a proactive role. Before offering cyberinsurance products to SMEs, they have to create awareness among them about cyber risks. A policy measure related to regulating *the role and liability of insurance providers and brokers in advising their clients on cyber security* (see “Best practices” policy measures) is relevant to SMEs as they aim to get a high-quality advice and trust their advisor. At the same time brokers and insurance companies have to understand what is their responsibility in this case.

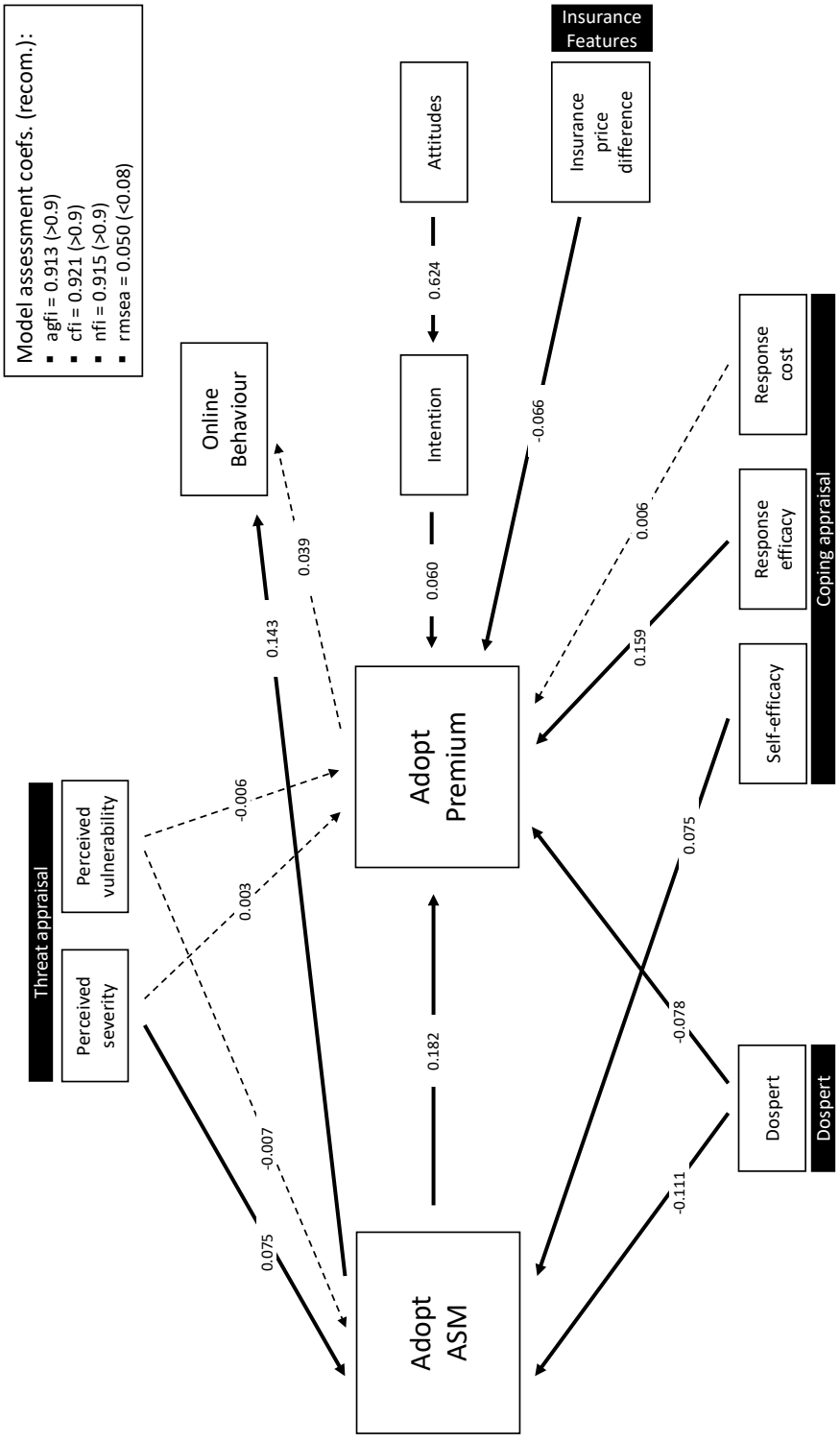

Figure 6.2: SEM model of cyberinsurance adoption

We also found out that cyber threats and the way companies deal with them are sensitive topics for SMEs. This fact can also explain why SMEs do not communicate with each other their actions related to cyber security. It could also slow down the penetration of security best practices within SME. Therefore, a policy measures on *establishing a security certification scheme for companies and promoting security awareness* could help SMEs to get a clear picture on their security state. This policy measure is also supported by Cihon *et al.* (2018): *"The regulation should clearly signal to firms that certification helps meet their cybersecurity 'duty of care', which, if a breach were to occur, would see firms enjoy better defense against tort liability and fines."*.

6.4.2 Component: Threat Appraisal

In regard to the *threat appraisal* component, we identified that SMEs are afraid of increasing digitalization and use of cloud technology as their data can be lost or leaked. In turn, that affects the trust of their clients and the company's reputation. Digitalization of the business is necessary to grow it, but at the same time is the main factor that makes SMEs vulnerable to attacks. Due to the increasing digitalization, companies also have to respond by increasing the level of technical protective measures to keep their data secure. These reasons together with the low probability of a cyber attack motivate SMEs to consider whether cyberinsurance could be a reasonable risk transfer strategy. In this case, a policy measure on developing *standard language for cyberinsurance policies* could help SMEs to better understand what residual risks they can transfer with cyberinsurance in addition to the existing countermeasures.

6.4.3 Component: Coping Appraisal

Regarding this component, cyberinsurance seems to be an attractive option 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, cyberinsurance provides complementary knowledge and assistance in dealing with a cyber incident. It is something that SMEs value since they usually do not have the personnel with the experience to deal with these kinds of situations. On the other hand, if an SME has the personnel with cyber security expertise and invested enough money in cyber security countermeasures and company's resilience, their motivation to get cyberinsurance is reduced. A policy measure regarding *legislation assigning financial costs to cyber events* will probably affect such companies and motivate them to consider cyberinsurance option. Various cyberinsurance providers offer services aiming to ensure that the company is compliant with existing regulations and fulfill necessary procedures in case of situations that potential could cause regulatory fines. However, both sides should understand each other and talk on a *standard language for cyberinsurance policies*.

7 Simulating policy effects with agent-based modelling

In order to simulate the effects of different types of policy interventions on overall risk, we developed a so-called agent-based model (ABM). In agent-based modelling, system-level effects are studied based on simulating the behaviour of individual agents and their interactions. We found that the various insurance policy options had positive but rather small influences. The combination of several policy options into a synergetic design provided results with more observable effects on the ecosystem level. The following is a summary of the full report (Sewnandan 2018).

Figure 7.1: The simplified ecosystem for the agent-based model (Sewnandan 2018).

7.1 Model design

In order to keep the complexity of the model manageable, we used a simplified version of the ecosystem and its agents as the basis for the model. This simplified ecosystem is shown in Figure 7.1.

For the agents in the simplified ecosystem, behavioural rules and parameters were defined as detailed in (Sewnandan 2018). At each “tick” of the model, representing a month in real time, agents observe their environment and execute actions. This includes decisions about purchasing insurance and/or investing in improved security. Individual security strengths are updated through (a) effectiveness reduction over time, and (b) new security investments. Security strength influences the risk of being attacked. Figure 7.2 shows the associated flow diagram.

The agent-based model was implemented in NetLogo, with an interface as shown in Figure 7.3.

The system-level variables we are interested in to study the effects of policy interventions are:

1. The average security strength in the ecosystem;
2. The global loss in the ecosystem (representing the inverse of resilience).

Using the model above, we investigated the ecosystem effects of the following insurance policy options:

7.1: CYBECO Policy Recommendations

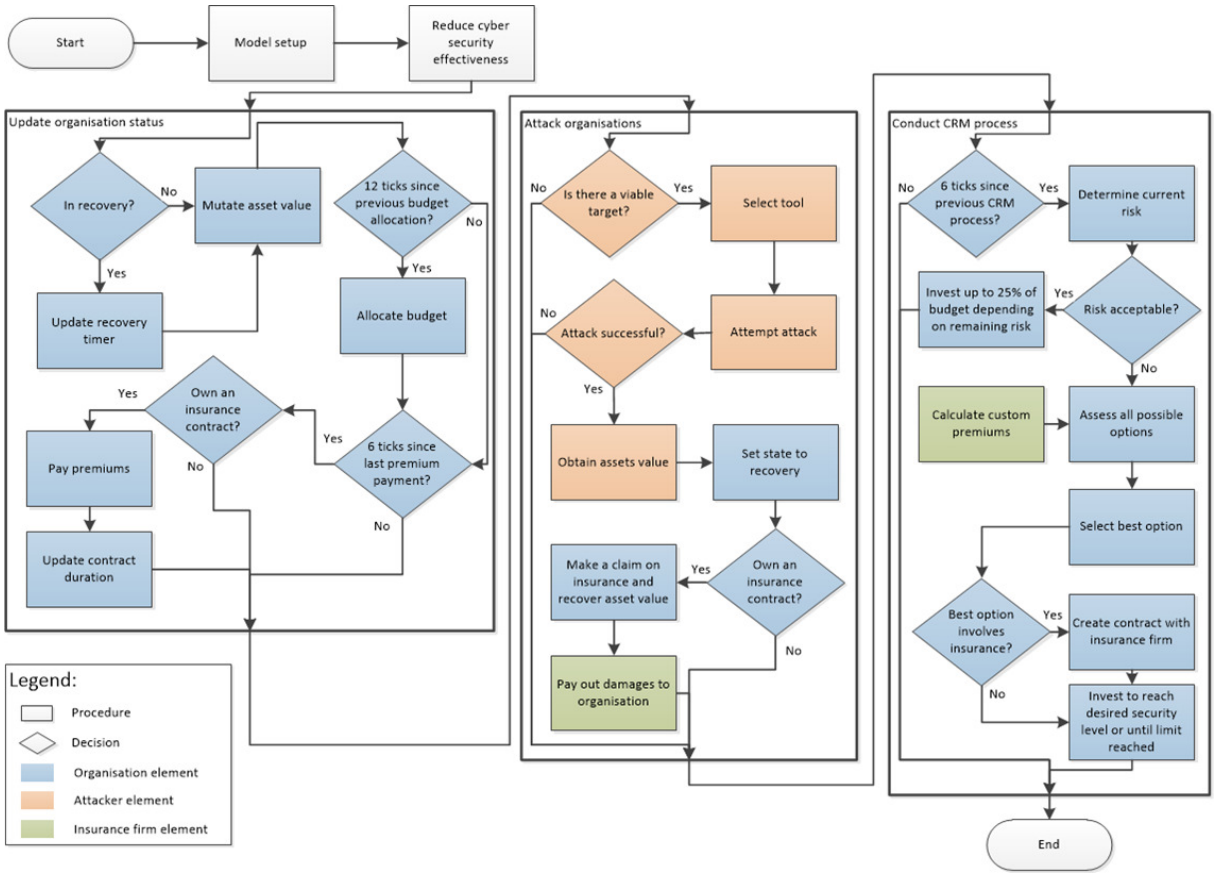

Figure 7.2: The flow diagram of the agent-based model (Sewnandan 2018).

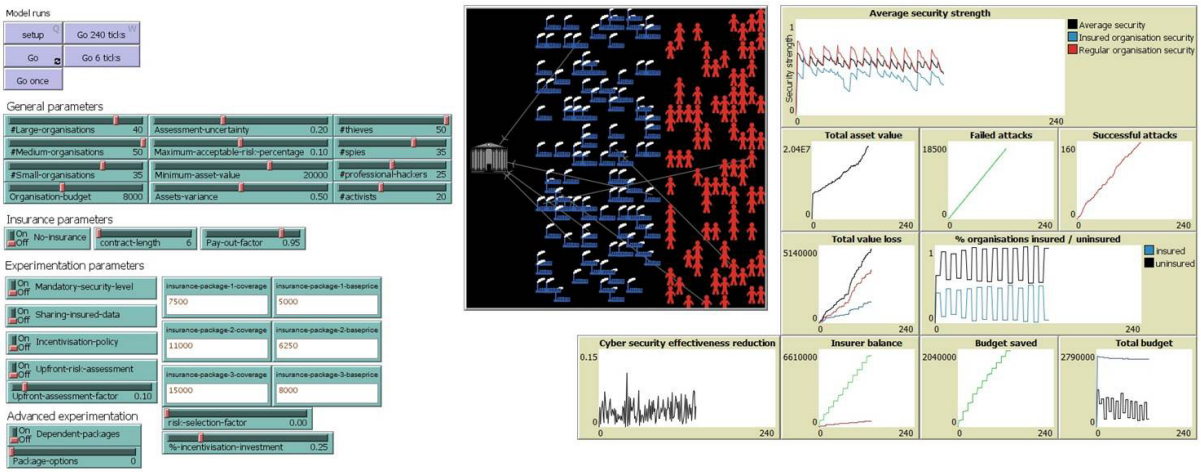

Figure 7.3: The interface of the agent-based model in NetLogo (Sewnandan 2018).

Package options the combination of maximum coverage and premium;

Contract length the duration of the insurance contract (6, 12 or 24 months);

Risk selection demanding minimum security levels, or increasing the premium for low-security clients;

Incentivisation lowering the premium for high-security clients;

Upfront risk assessment requiring that the client do a certain type of risk assessment first;

Sharing cyber security control information providing clients with threat information based on the whole insurance portfolio;

Requiring organisations to maintain their security level demanding that initial security levels are maintained to ensure coverage.

We also investigated the effects in a synergy experiment combining the options of risk selection, incentivisation, and sharing cyber security control information.

7.2 Results

Figure 7.4 shows the effect of the different policy options on the global security strength. It can be seen that the effects of the different policy options on global security strength are relatively small, with the synergy experiment providing the best result.

Figure 7.5 shows the effect of the different policy options on the global value loss. Again the differences are small. The synergy experiment is somewhere in the middle here. This suggests that although the combination of policy options improves overall security, it does not necessarily improve resilience. This is because high-risk organisations may not purchase insurance when risk selection and incentivisation are in place.

Figure 7.6 shows the number of insured organisations per policy option (out of 125 organisations in total). It can be seen that the synergy experiment has a relatively low percentage of insured organisations. This is because the combined policy options make insurance less attractive for some (high-risk) organisations, thereby reducing adoption but improving ecosystem-level security.

7.3 Conclusions and discussion

Based on the agent-based model and its results described above, a few conclusions can be drawn.

1. Under the assumptions in this experiment, the overall effect of individual policy options on security strength and resilience at thee ecosystem level is small.
2. Combining different policy options increases the effect on security strength, but does not necessarily improve resilience.
3. Cyberinsurance policy interventions can only have a large effect on the ecosystem in case of widespread adoption under the baseline condition. Some policy measures will actually be effective precisely by reducing the number of insured organisations, for example when avoiding moral hazard through risk selection.

7.1: CYBECO Policy Recommendations

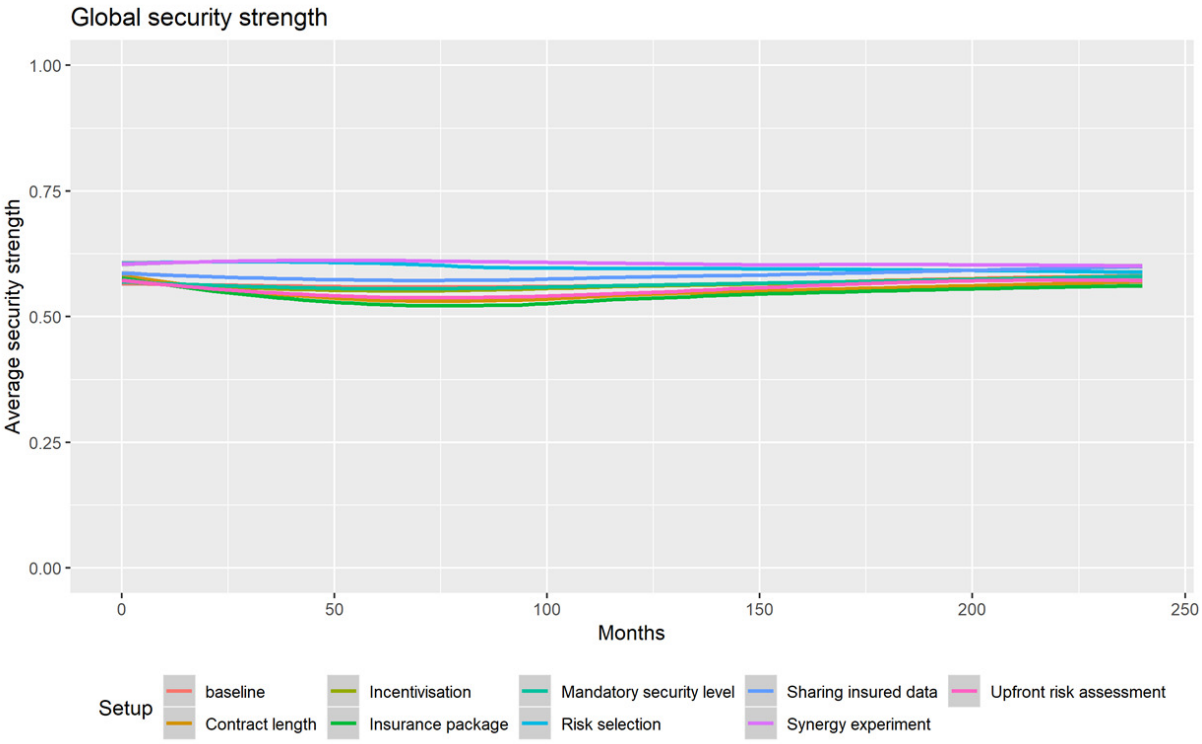

Figure 7.4: Effects of policy options on global security strength (Sewnandan 2018).

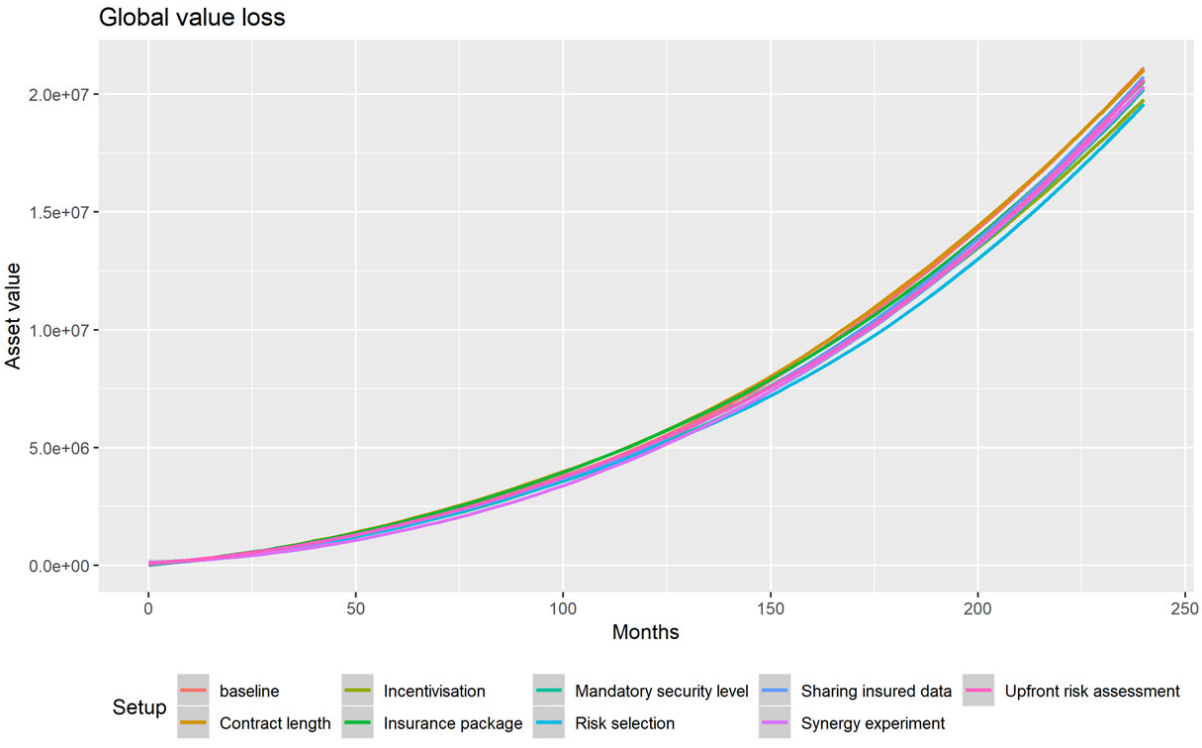

Figure 7.5: Effects of policy options on global value loss (Sewnandan 2018).

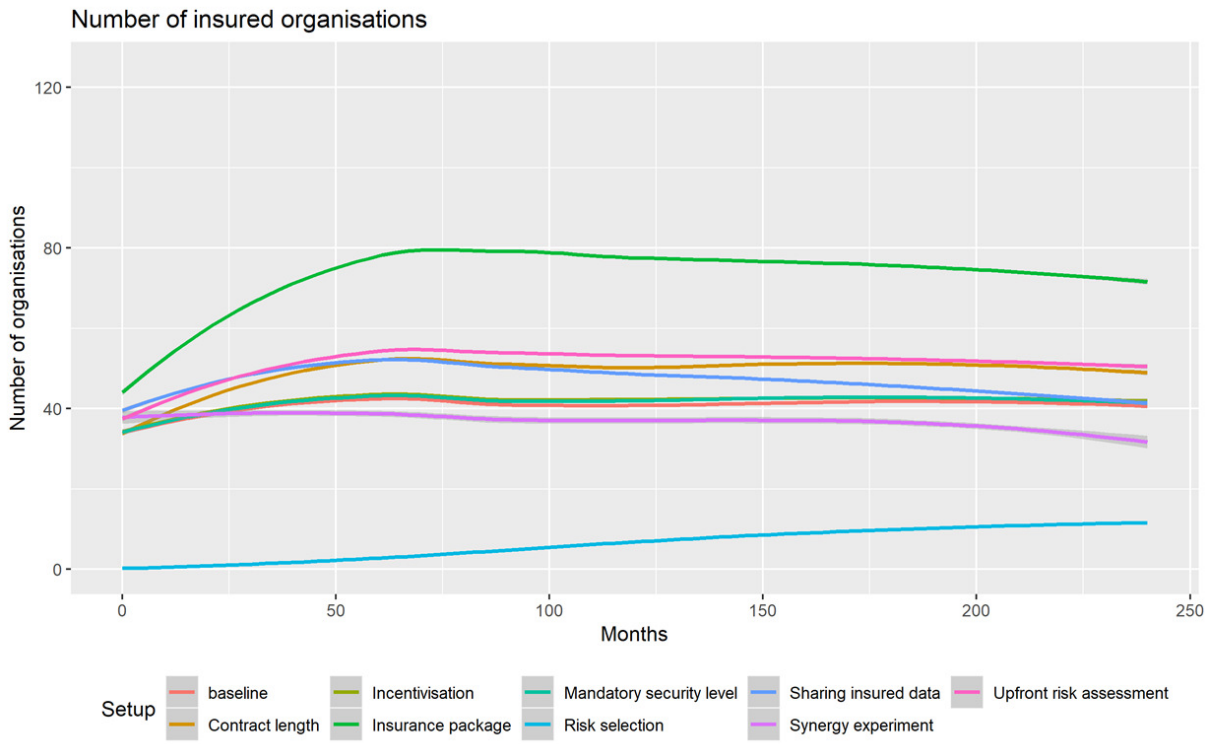

Figure 7.6: The number of insured organisations per policy option over time (Sewnandan 2018).

As in any agent-based modelling exercise, assumptions had to be made regarding behavioural structures of the agents as well as model parameters. The model has been run with different variations of parameters, and the insights above are relatively robust. Nevertheless, behavioural rules that form the based of an agent-based model will still serve as basic assumptions without which a model cannot be created in the first place. Further studies can investigate the effect of different assumptions on the resulting ecosystem patterns.

In terms of policy recommendations, we can derive that (a) policy makers should be aware that, depending on the circumstances, their key role may be in preventing negative effects of cyberinsurance rather than stimulating positive ones; and (b) policy measures that improve resilience may weaken overall security, because increasing the number of insured organisations may worsen the moral hazard problem. This trade-off is a key factor in decision-making. In addition, balancing the positive effects of policy measures with the ethical considerations in chapter 3 should be taken into account.

8 Discussion on policy recommendations

This chapter summarises the findings of our work on the governance of cyberinsurance, relates those to the discussions at the Lorentz seminar we organized, and provides a final discussion on policy options and associated recommendations.

8.1 Summary of findings

In this document, we focused on how the cyberinsurance ecosystem functions, how different interventions would influence the ecosystem, and which governance options are currently underexplored. We found that:

Ch. 3 Among the goals of the main actors in the cyberinsurance ecosystem, some require more attention from the policy makers and regulatory side. Specifically, the *relation between insureds and incident response providers* is currently not regulated and, in case the incident response company is affiliated with the insurer, it is an open question in whose favor this company might act when handling incidents covered by cyberinsurance. Also other goals like *increasing an overall level of security* for a governmental actor or *getting advice on security investments* and *getting coverage for possible losses related to cyber risk* could benefit from additional policy developments, as the current policy measure options do not cover it well.

Ch. 3 In addition to stakeholder goals, policy measures should take ethical considerations into account, including moral hazard, responsibility for collective values, and fairness.

Ch. 4 Existing cyber security regulations are mostly developed in the part related to *creating financial costs to cyber events* that can contribute to wider adoption of cyberinsurance. Most of the regulations set certain limits for financial penalties in case of a breach event, but, for example, the NIS directive leaves the possibility to define penalties to local authorities. The results of our study with SMEs suggest that the policy measure related to creating financial costs to cyber events will probably affect such companies and motivate them to consider cyberinsurance.

Ch. 4 There is no agreement on the level of granularity for security requirements in the investigated directives. This part would need more work from policy analysis and security experts on *setting certain level of cyber security requirements for organizations*.

Ch. 5 The ecosystem within companies is complex and the decision-making process varies across businesses. This chapter focused on the decision-making process at the company level. The findings suggest that policy measures related to *standardization of insurance policy coverage and implementation of best practices* could be beneficial to help address mistrust in insurers from companies, and/or boost cyberinsurance adoption. Policy measures increasing *anonymised data sharing* would be beneficial in regard to achieving greater awareness around cyber risk and improving practice. Lastly, we need to facilitate research aiming at understanding organisational structures better that could be beneficial for effective policy.

Ch. 6 Cyber threats and their mitigation is sensitive information for SMEs and, therefore, its communication is probably hindered, which slows down the adoption of security best practices and cyberinsurance among companies. Policy developments related to *establishing a security certification scheme for companies and promoting security awareness* could support SMEs in getting a clear vision of their level of security.

Ch. 6 Policy advancement on establishing a *standard language for cyberinsurance policies* could support SMEs in better understanding what residual cyber risks they can transfer to cyber insurers as a supplement to the implemented security controls. Such standard language would also help insureds and insurers to better understand each other.

Ch. 7 The key role of policy makers, depending on the circumstances, may be in preventing negative effects of cyberinsurance rather than stimulating positive ones. Policy measures improving the resilience of the ecosystem may weaken overall security, as increasing the number of insureds may worsen the moral hazard problem.

8.2 Results from Lorentz seminar

In addition to the research done within CYBECO, we obtained additional considerations on policy measures from our dissemination event. The CYBECO project organized the Lorentz seminar on "Cyberinsurance and its contribution to cyber risk mitigation" from March 25 until March 29 in Leiden, The Netherlands, in cooperation with external experts.[1] The seminar included working groups on the cyberinsurance market as well as on cyberinsurance policy. Key suggestions that may impact policy recommendations are discussed below.

In the seminar and its working groups, the following policy gaps were identified:

Silent cyber Silent cyber refers to cyber threats and incidents that are covered under traditional insurance policies, without being explicitly included (but neither being excluded). What to do about silent cyber is a policy-relevant question, because silent cyber may entail uncertainty and financial risks to insurance companies. The UK explicitly asked insurance companies to investigate their situation with respect to silent cyber.

Fines There is considerable uncertainty with respect to the insurability of fines. Although in some countries this may be explicitly allowed or forbidden, in other countries it is unclear whether (GDPR) fines can be insured. Whether fines can be insured may depend on specific characteristics / types of fines. It is unclear who would bring this to court to create clarity; none of the stakeholders in the ecosystem appears to have incentives to do so.

Response Most incident response services included in cyberinsurance offerings focus on the incident within the company. In terms of societal benefits, it would be beneficial if what is learnt from the instantiation of the incident within the specific company is also leveraged in cross-company incident response, e.g. notification of others who may be vulnerable to the same threat. Such services could be stimulated by the government.

[1] https://www.lorentzcenter.nl/lc/web/2019/1096/info.php3?wsid=1096&venue=Oort

Sharing Stakeholders perceive legal boundaries for information sharing (e.g. in relation to privacy). It is therefore important to clarify under what conditions (incident) information can be shared. Cyberinsurance policy measures should be connected to cybersecurity information sharing policy.

Specific points of attention for cyberinsurance governance were also highlighted:

Incentives If this is deemed beneficial for resilience, there are different ways of encouraging cyberinsurance adoption. This ranges from making cyberinsurance mandatory for specific domains via nudging to simply providing information and awareness.

Brokers Brokers may play a key role in facilitating specific changes to insurance policies. Governance of cyberinsurance should specifically address the role of the broker.

Sectors Policy measures may be designed for general application or for specific sectors. Even for general measures, specific sectors may be used as a testbed / niche.

In addition, it was suggested that for all policy gaps and associated measures, policy makers should be aware that some stakeholders in the ecosystem may benefit from the gaps / lack of measures, and may therefore openly or secretly oppose changes.

8.3 Final recommendations

To facilitate the adoption of the results discussed, we end this deliverable with specific recommendations addressing cyberinsurance adoption and development for European and national-level policy makers. We refer to the specific chapters/sections that informed these recommendations.

1. Help responsible cyberinsurance adoption through:
    a) Unification of existing regulations in relation to financial penalties for breaches. Esxisting cyber security and data protection regulation have varied conditions regarding financial penalties for regulation breaches and companies may not have a complete vision of the consequences related to non-compliance (see Section 4.1),
    b) Clarifying the position in relation to the insurability of fines created by cyber security regulations, and
    c) Developing a standard in information security best practices that cyberinsurance providers can use as baseline security requirements for cyberinsurance policies (see Section 3.1.5). As discussed in Chapter 4, most existing cyber security regulations do not clearly define security requirements. They need to be flexible and take into account the changing nature of cyber security risks and advances in cyber security protection measures (see discussion in Section 5.5). Creating a specific standard of security recommendations for cyberinsurance and linking it to a certification scheme could help companies in getting a clear picture of their security state and how they can be insured against cyber risks (more discussion in Section 3.1.5 and 6.4.1).
2. Connect information sharing and cyberinsurance policy and initiatives by:
    a) Investigating the situation regarding incident handling services. As discussed in Section 3.4, there is no clear position about relations between companies and incident management providers (including those recommended by insurers). We do not

know in whose interests these providers act when working in cooperation with insurers. However, such services are highly valued by SMEs as shown in Section 6.4.3,

b) Facilitating the exchange of information about cyber incidents handled by cyber security incident response companies with other organizations that could be affected by the same problem (see Section 8.2),

c) Encouraging the publication of data breach notifications to DPAs under the GDPR as discussed in Section 3.1.4. This facilitates the improvement of efficiency of insurance pricing, which encourages further adoption.

d) Developing and communicating guidelines for stakeholders regarding sharing information about incidents with respect to privacy and other relevant aspects (see Section 8.2).

3. Supervise the situation related to silent cyber coverage in traditional insurance lines at the European level (see Section 8.2) by:

   a) Monitoring the level of silent coverage of cyber risks in traditional insurance products,

   b) Facilitating the development of the standard language for cyber risk and what can or cannot be covered in this respect, and

   c) Promoting cyber exclusions in traditional insurance products to limit silent cyber coverage.

All these policy options may contribute to the goals of global security strength and resilience. However, the two goals are not necessarily aligned, and they may also conflict with values such as fairness. Therefore, striking the right balance between the main goals and ethical considerations is key when implementing policy around cyberinsurance. We suggest focusing on responsible adoption rather than simply stimulating the take-up of cyberinsurance per se.

Bibliography

AIG. 2017. *CyberEdge Playbook: A broker guide to selling cyber insurance*.

Anderson, R. 2001 (Dec). Why information security is hard - an economic perspective. *Pages 358–365 of: Seventeenth Annual Computer Security Applications Conference*.

Arant, Peter J. 2016. Understanding Data-Breach Liability: The Basics Every Attorney Should Know. *Oklahoma Bar Journal*, **87**(11-4).

Baker, Tom. 2002. Risk, insurance, and the social construction of responsibility. *Pages 33–51 of: Embracing risk: the changing culture of insurance and responsibility*. University of Chicago Press Chicago, IL.

Bershidsky, Leonid. 2019. Zurich Policyholder Dispute Highlights Danger of Calling Out Cyber Attackers: Opinion. *Insurance Journal*.

Brice, William B. 1994. Brittish Government Reinsurance and Acts of Terrorism: The Problems of Pool Re. *U. Pa. J. Int'l Bus. L.*, **15**, 441.

Briggs, Pam, Branley, Dawn, Nicholson, James, Coventry, Lynne, Vila, Jose, & Gomez, Yolanda. 2018a. *D6.1: Economic Experiments Concept Note*.

Briggs, Pam, Branley, Dawn, Nicholson, James, Coventry, Lynne, Vila, Jose, & Gomez, Yolanda. 2018b. *D6.3: Report with Findings of Experiments and Policy implications*.

Briggs, Pam, Branley-Bell, Dawn, & Gomez, Yolanda. 2019. *Testing a predictive model of cyberinsurance adoption (Working paper)*.

Burke, W. Warner, & Litwin, George H. 1992. A causal model of organizational performance and change. *Journal of management*, **18**(3), 523–545.

Chew, Elizabeth, Swanson, Marianne, Stine, Kevin, Bartol, Nadya, Brown, Anthony, & Robinson, Will. 2008. *Performance measurement guide for information security*. Tech. rept. National Institute of Standards and Technology.

CIAB. May 2017. *Cyber insurance market watch survey*.

Cihon, Peter, Guitierrez, Glenda Michel, Kee, Sam, Kleinaltenkamp, Moritz, & Voigt, Thanel. 2018. *Why certify: increasing adoption of the proposed EU Cybersecurity Certification Framework*.

Contreras, Ricardo B. 2011. Examining the Context in Qualitative Analysis: The Role of the Co-Occurrence Tool in ATLAS. ti. *Newsletter*, **2011**, 2.

Doyle, Aaron. 2011. Introduction: Insurance and Business Ethics. *Journal of Business Ethics*, **103**(1), 1–5.

European Commission. *What is an SME? - European Commission*.

Fauntleroy, JC, Wagner, Ryan R, & Odell, Laura A. 2015. *Cyber Insurance-Managing Cyber Risk*. Tech. rept. Institute for Defense Analyses Alexandria VA.

Floyd, Donna L, Prentice-Dunn, Steven, & Rogers, Ronald W. 2000. A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, **30**(2), 407–429.

Greco, Gian Maria, & Floridi, Luciano. 2004. The tragedy of the digital commons. *Ethics and Information Technology*, **6**(2), 73–81.

Hayel, Yezekael, & Zhu, Quanyan. 2015. Attack-aware cyber insurance for risk sharing in computer networks. *Pages 22–34 of: Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9406.

Heidt, Margareta, Gerlach, Jin, & Buxmann, Peter. 2019. A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions. *In: Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Heimer, Carol A. 2003. Insurers as moral actors. *Risk and morality*, 284–316.

ISO/IEC. 2019. DIS 27102 - Information technology — Security techniques — Information security management guidelines for cyber insurance.

Kesan, Jay P, & Hayes, Carol Mullins. 2017. Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment.

Kissel, Richard. 2013. Glossary of key information security terms. *NIST Interagency Reports NIST IR*, **7298**(3).

Kok, Matthijs, Vrijling, JK, Van Gelder, PHAJM, & Vogelsang, MP. 2002. Risk of flooding and insurance in the Netherlands. *Pages 146–154 of: Proceedings of the Second International Symposium on Flood Defence*. Science Press, New York, NY, USA.

Kuypers, Marshall A, Maillart, Thomas, & Pate-Cornell, Elisabeth. 2016. *An empirical analysis of cyber security incidents at a large organization*.

Levi-Faur, David. 2011. *Handbook on the Politics of Regulation*. Edward Elgar Publishing.

Marotta, Angelica, Martinelli, Fabio, Nanni, Stefano, Orlando, Albina, & Yautsiukhin, Artsiom. 2017. Cyber-insurance survey. *Computer Science Review*.

Marsh, HM Gevernment &. March 2015. *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*.

Martinez Bustamante, Inés. 2018. *Drivers and impediments for cyber insurance adoption among Dutch SMEs*. M.Phil. thesis, Delft University of Technology.

Mentzer, John T, DeWitt, William, Keebler, James S, Min, Soonhong, Nix, Nancy W, Smith, Carlo D, & Zacharia, Zach G. 2001. Defining supply chain management. *Journal of Business logistics*, **22**(2), 1–25.

Minty, Duncan. 2018. *Personalisation – could it take insurance into a digital winter?* `https://ethicsandinsurance.info/2018/03/08/personalisation/`.

Nieuwesteeg, Berenold, van Eeten, Michel, & Faure, Michael. 2018a. *Scientific research data brreache notification obligation*.

Nieuwesteeg, Bernold, Visscher, Louis, & de Waard, Bob. 2018b. The Law and Economics of Cyber Insurance Contracts: A Case Study. *European Review of Private Law*, **26**(3), 371–420.

OECD. 2017a. *Enhancing the Role of Insurance in Cyber Risk Management*.

OECD. 2017b. *Enhancing the Role of Insurance in Cyber Risk Management*. Tech. rept. OECD.

Palmer, Daniel E. 2007. *Insurance, Risk Assessment and Fairness: An Ethical Analysis*. Pages 113–126.

Pieters, Wolter. 2018. On Security Singularities. *Pages 80–88 of: Proceedings of the 2018 New Security Paradigms Workshop*. ACM.

Pieters, Wolter. 2019. Security. *In: Routledge Handbook of Philosophy of Engineering*. Routledge.

Regan, Priscilla M. 2002. Privacy as a Common Good in the Digital World. *Information, Communication & Society*, **5**(3), 382–405.

Renaud, Karen, Flowerday, Stephen, Warkentin, Merrill, Cockshott, Paul, & Orgeron, Craig. 2018. Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security*, **78**, 198–211.

Robinson, Neil. 2012. Incentives and Barriers of the Cyber Insurance Market in Europe.

Romanosky, Sasha. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, **2**(2), 121–135.

Romanosky, Sasha, Ablon, Lilian, Kuehn, Andreas, & Jones, Therese. 2017. Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *In: Proceedings of the 16th Workshop on the Economics of Information Security (WEIS)*.

Sewnandan, Jhoties. 2018. *Analysing the impact of cyber insurance on the cyber security ecosystem: Utilising agent-based modelling to explore the effects of insurance policies*. M.Phil. thesis, Delft University of Technology.

Stoneburner, Gary, Goguen, Alice Y, & Feringa, Alexis. 2002. Risk management guide for information technology systems.

Tosh, Deepak K, Vakilinia, Iman, Shetty, Sachin, Sengupta, Shamik, Kamhoua, Charles A, Njilla, Laurent, & Kwiat, Kevin. 2017. Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance. *Pages 519–532 of: Decis. Game Theory Secur.* Springer International Publishing.

Turoff, Murray, & Plotnick, Linda. 2012. The ISCRAM future threat Delphi: Nostradamus revisited. *In: 9th International ISCRAM Conference Proceedings*.

US DHS. 2012. *Cybersecurity Insurance Workshop Readout Report*.

van der Wagen, Wytske, & Pieters, Wolter. 2019. The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, 1477370818812016.

Weishäupl, Eva, Yasasin, Emrah, & Schryen, Guido. 2018. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, **77**, 807–823.

Woods, Daniel, & Simpson, Andrew. 2017. Policy measures and cyber insurance: a framework. *Journal of Cyber Policy*, **2**(2), 209–226.

Yang, Zichao, & Lui, John C.S. 2014. Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Perform. Eval.*, **74**, 1–17.