THE LAW & ECONOMICS OF CYBER INSURANCE CONTRACTS: A CASE STUDY

Bernold Nieuwesteeg, Louis Visscher & Bob de Waard

***

We combine cyber risk literature with insurance law and economics literature to study cyber insurance contracts. We aim to explore to what extent current cyber insurance contracts contribute to social welfare, both theoretically and empirically. First, we discuss main trade-offs in insuring cyber risk within a theoretical framework. This framework also includes account strategic behavior of market participants and impediments for market growth that result from the complex dynamics of cyber risk. Subsequently, a case study in the Netherlands compares the theoretical expectations with the actual state of cyber insurance contracts, prices and market participants. The results suggest that insurers currently halt between two options: either a strategy of rigorous market penetration with easily accessible and attractive insurance products, or a strategy of significant hedging of correlated risks that reduces the potential of cyber insurance. We aim to assist lawyers, legal councils and judges when drafting or reviewing actual cyber insurance contracts.

Key words: cyber risk; law and economics; insurability; cyber insurance; contracts

***

INTRODUCTION

In this contribution, we combine cyber risk literature with insurance law and economics literature to study cyber insurance contracts. It aims to explore to what extent current cyber insurance contracts for Small and Medium Enterprises (SMEs) contribute to social welfare, and what options exist to improve these contracts to utilize the potential of cyber insurance. Therefore, we first discus the potential of insuring cyber risk to reduce market failures in cyber security. Hereafter, a theoretical framework for cyber insurance contracts, prices, and strategies of market participants is formulated. Within this framework, we discuss trade-offs to be made in order to attain a cyber insurance market that can contribute to social welfare. Simultaneously, it evaluates impediments to socially ideal situations including strategic behavior of the insured and the systemic instability of cyber risks, leading to expectations on

the insurers' strategies regarding the design of insurance contracts. In order to compare the expectations from the theoretical framework with the actual state of cyber insurance contracts, we empirically analyze the emerging field of cyber insurance for SMEs by reviewing actual cyber insurance contracts through a case study in the Netherlands. Insurance contracts were requested from all insurers offering cyber insurance on the Dutch market. Six different SMEs, varying in size and Internet dependency, are included. This setup allows for an analysis and comparison of insurance contracts of different insurers for alternative types of SMEs, and to analyze prices and the number of market participants. Hence, the Dutch case study provides a way to observe how insurance companies design contracts and respond to challenges of the insurability of cyber risks, which include the correlated nature of cyber risks and the lack of actuarial data in this particular field.

The Authors performed this study because research on the law and economics of cyber insurance contracts is scarce, but important. The limited empirical research on the content of cyber insurance contracts that is available in practice concerns case studies in the United States more than a decade ago.[1] Obviously, the information and communication technology landscape has changed considerably in the past decade. Drivers for the evolution of the cyber landscape include the development of smartphones, Big Data, Internet of Things and the availability of more easy to use cybercrime tools. Hence, hypotheses and results from the early 2000s that concern the state and development of cyber insurance deserve an update. Besides studying the development of the cyber insurance market as such, insurance law theory can be developed further by learning from the new structure and dynamics of the cyber risk market. In this way, we aim to contribute to the overarching literature on the insurability of risks and to add a possible important cornerstone to the current literature on cyber insurance. Studies from this field focus mainly on the insurability and description of cyber risk but do not take into account the actual analysis of the policies and premiums itself.[2] Hence, from an academic perspective, this research contributes to literature on cyber

[1] Perry Luzwick, If Most of Your Revenue is From E-commerce, Then Cyber-Insurance Makes Sense, 2001 Computer Fraud and Security 3, 16-17 (1999); Robert H. Jerry II & Michele L. Mekel, Cybercoverage for Cyber-Risks: An Overview of Insurers' Responses to the Perils of E-Commerce, Conn. Ins. L.J. 8, 7-36 (2001); Jay P. Kesan, Majuca P. Ruperto & William J. Yurcik, The Economic Case for Cyberinsurance, Working paper, University of Illinois, IL. (2004). There are more recently published updates about the state of the cyber insurance market, but they do not explain the methodology followed, and cannot be qualified as scientific research, see for instance: Rob Van de Laar, Cyberrisico's: Meer dan ICT, AMPlus 10, 49-52 (2013).

[2] Rainer Böhme & Galina Schwartz, Modelling cyber-insurance: Towards A Unifying Framework, Paper presented at 2010 9th Annual Workshop on the Economics of Information Security, Harvard Business School, Boston, MA. (2010); Philip Rawlings, Cyber Risk: Insuring the Digital Age, Queen Mary School

insurance law as well as to literature regarding insurability for cyber-risks. From a law practice perspective, this research can inform courts which want to take economically sound decisions with regard to cyber insurance law. It is crucial for lawyers and insurance contract drafters to be aware of the economic effects of insurance law, because judges may scrutinize cyber insurance contracts from a law and economics perspective. Lawyers, general councils and judges can be aided by a structured summary of industry wide cyber insurance contracts. We therefore give a legal overview of insurance contracts, discuss directions for a socially ideal set up of those contracts, discuss strategic behavior by insurance companies and observe to what extent those contracts are enhancing social welfare.

Based on our case study, we find that insurers use different approaches to respond to the specific challenges of cyber security. On the one hand, some of the behavior of insurers is aimed at gaining market share and eventually market size. A bigger market results in more data about cyber security risks. This is attractive for consumers and this enhances social welfare. On the other hand, some elements within contracts are primarily aimed at reducing (private) risk for the insurer, thereby lowering the likelihood that a market will develop. Thus, insurance companies seem to be halting between two options, gaining market share while on the other hand reducing and managing their own risk. This currently hinders the cyber insurance market from reaching its full potential in contributing to social welfare. A possible explanation for these findings is that traditional insurers, which might not have adequate experience to insure cyber risks, offer the cyber risks insurance. Cyber risks are a completely different category of risks and have a different lifecycle than other risks that those companies traditionally insure. A last important finding is that insurers in general use very little 'moral hazard measures'.[3] These are requirements the insurer gives to the insured in order to decrease the likelihood of claims. This has unused potential, since moral hazard measures are considered welfare enhancing.[4]

---

of Law Legal, research paper 189 (2015); ENISA, Incentives and Barriers of the Cyber Insurance Market in Europe, Report for the European Commission (2012); Christian Biener, Martin Eling & Jan H. Wirfs, Insurability of Cyber Risk: An Empirical Analysis, 40 The Geneva Papers 1, 131-158 (2014); Mark Greisiger, Cyber Liability & Data Breach Insurance Claims - A Study of Actual Payouts for Covered Data Breaches, Gladwayne, PA: NetDilligence (2011).

[3] An example of a moral hazard measure that the Authors did observe is the requirement to make a back up every week.

[4] That is, when the social marginal benefits of these moral hazard measures are larger than the social marginal costs. Because the insurer potentially has more information about the market than the insured, he is in a better position to judge which investments are efficient.

The remainder of this contribution is organized as follows. In section II we briefly describe cyber risk and various market failures that frustrate a socially efficient allocation of cyber security investments. In the general literature (not specifically aimed at cyber risk), various potential remedies for these market failures are proposed, insurance being one of them. We subsequently discuss the potential of cyber insurance to contribute to social welfare. In section III, we investigate hurdles that need to be overcome in cyber insurance contracts, prices, and competition, in order for cyber insurance to contribute to social welfare. This section analyzes coverage clauses, prices, competitors, adverse selection, reverse adverse selection and moral hazard measures. For each element, trade-offs and impediments for attaining a socially ideal situation are discussed. Moreover, this section formulates expectations on the design of cyber insurance contracts for Dutch SMEs, given the impediments for growth. Section IV describes the setup for the case study. We collected information on actual cyber insurance policies from nine insurers operating on the Dutch market, for six different potential insured SMEs with varying characteristics. Section V presents the results of the case study. This section analyzes how the offered policies compare to the expectations from the theoretical framework. Subsequently, contracts are discussed on various aspects including premiums, deductibles, caps, coverage, moral hazard- and adverse selection clauses, and requesting procedures. Section VI draws conclusions from the empirical analysis and provides ideas about how cyber insurance policies may be improved, and give suggestions for future research.

II. Cyber Risk and The Potential of Insuring It

A. Cyber Risk

The digital economy is a driver for economic growth. For instance, the usage of information technology has added 21% to the GDP growth of developed countries between 2006 and 2011.[5] Organizations increasingly use, and depend on, information technology products. This increased dependence on information technology has created a new hazard: cyber risk. We define cyber risk as the potential physical harm (to persons or property) and loss of profits due to malfunction of digital systems or corrupted data. The potential impact on society is large because information systems are interdependent. This can cause cascade effects,

[5] Matthieu Pélissié du Rausas, Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity, McKinsey&Company (2011), http://www.mckinsey.com/insights/high_tech_telecoms_Internet/Internet_matters (accessed 21 March 2016).

meaning that an incident can quickly spread among the users of the information system. Cyber risk hence is a systemic risk. For example, an error in a cloud computing service could quickly spread among all users, with potential catastrophic consequences.[6]

Cyber risk can be decomposed to *threat*, *vulnerability* and *impact* .[7]

- Threat concerns the probability that the potentially damaging event happens. This Article considers three types of threats: cybercrime, human errors and system failures.
- Vulnerability concerns the likelihood that once a threat materializes, losses occur. In so-called resilient systems, threats can take place without causing loss. Automatic back-ups and proper firewalls for example can avoid losses due to threats such as accidental deletion of files resp. virus attacks.
- Impact regards the losses due to the incident. Two important distinctions are made:
    - First party damage is damage at the organization that owns the information technology system.[8] Third party damage is damage at other organizations affected by the manifestation of cyber risk. In a situation of interdependent information systems of multiple third parties, the value of the assets of third parties probably exceeds the value of the first party. Third party damage then outweighs first party damage. This is especially relevant for SMEs, which have relatively limited assets but may cause substantial third party damage.
    - First order damage equals the direct costs organizations incur when a cyber incident occurs. A few examples: organizations can lose personal or company data through hacking, or failing hardware and software or mistakes of employees can interrupt their business.[9] Second order damage is the negative effect of an incident once it becomes public,[10] for example reputation damage.[11] Another example is being fined for not

[6] Andreas Haas & Annette Hofmann, Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit, FZID Discussion Paper No.74, Hohenheim (2013).

[7] ISO, Information Technology - Security Techniques - Information Security Risk Management, ISO/IEC 27005 (2011), https://www.iso.org/obp/ui/#iso:std:56742:en (accessed 21 March 2016); Yacov Y. Haimes, On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, 26 Risk Analysis 2, 293-296 (2006); Eric J. Byres & Justin Lowe, The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems, Paper presented at 2004 VDE Congress, Berlin (2004).

[8] Daniel Schwarcz & Peter Siegelman, eds., Research Handbook on the Economics of Insurance Law, Cheltenham, UK & Northampton, MA: Edward Elgar Publishing (2015).

[9] James J. Cebula & Lisa R. Young, A Taxonomy of Operational Cyber Security Risks, Software Engineering Institute, Carnegie Mellon University (2010), http://www.sei.cmu.edu/reports/10tn028.pdf (accessed 21 March 2016).

[10] Tridib Bandyopadhyay, Vijay S. Mookerjee & Ram C. Rao, A Model to Analyze the Unfulfilled Promise of Cyber Insurance: The Impact of Secondary Loss, Working paper, University of Texas, TX (2004).

[11] Jennifer. R. Veltsos, An Analysis of Data Breach Notifications as Negative News, 75 Business

notifying breaches to a data breach notification authority. Second order damage is more difficult to measure than first order damage and hence harder to transfer to a third party such as an insurer. This could result in suboptimal claim behavior in the case of cyber insurance.[12]

B. Market Failures in Cyber Risk

Parties can take care measures to reduce (the costs of) cyber risk. Law and economics literature labels care as 'socially optimal' if the additional social ('marginal') costs of taking more care equal marginal benefits thereof.[13] The socially optimal level of cyber risk hence will be reached if socially optimal care is taken. Care measures can be targeted at all three elements of cyber risk: threat, vulnerability and impact. Some threats tend to be relatively immune for care measures, such as malware attacks that seem to occur independent of one's care level,[14] while the likelihood of materialization of other threats such as human failures can be reduced by taking actions such as cyber security awareness training courses. Vulnerability can be reduced by, among others, regularly updating firewalls, virus scanners and operating systems.[15] Impact can be reduced by for instance segmentation of valuable assets,[16] or by mitigation measures after the incident,[17] such as notification of the breach to other potentially affected parties.[18]

Within cyber security, the social costs and benefits differ from the private cost and benefits so that the market will not reach the social optimum by itself.[19] Positive externalities exist when third parties benefit from the investments of another party. This results in

---

Communication Quarterly 2, 192-207 (2012).

[12] Bandyopadhyay et al., supra note 10.

[13] See the following publications for an extensive discussion on this topic: Steven Shavell, Foundations of Economic Analysis of Law. Cambridge, MA: Belknap Press of Harvard University Press (2004); Robert Cooter & Thomas Ulen, Law and Economics, Boston, MA: Pearson Addison Wesley (2004); Hans-Bernd Schafer & Claus Ott, The Economic Analysis of Civil Law, Cheltenham, UK: Edward Elgar Publishing (2005); Michael G. Faure, Tort Law and Economics, Cheltenham, UK: Edward Elgar Publishing (2009).

[14] Samaneh Tajalizadehkhoob, Hadi Asghari, Carlos Gañán & Michel van Eeten, Why them? Extracting Intelligence About Target Selection from Banking Trojans, Paper presented at 2014 13th Annual Workshop on the Economics of Information Security, Pennsylvania (2014).

[15] CERT-UK & GCHQ, Common Cyber Attacks: Reducing the Impact. UK: Crown (2015).

[16] Pramod Pandya, Local Area Network Security, in J. R. Vacca, ed., Network and System Security, second edition, Waltham, MA: Syngress (2014).

[17] Faure, supra note 13.

[18] Bernold F. H. Nieuwesteeg, The Legal Position and Societal Effects of Security Breach Notification Laws, Amsterdam: Delex (2014).

[19] Ruperto P. Majuca, William Yurcik & Jay P. Kesan, The Evolution of Cyberinsurance, Arxiv (2006), http://arxiv.org/abs/cs/0601020 (accessed 21 March 2016).

underinvestment, because private benefits are smaller than social benefits.[20] When an increase in care level of a single organizations negatively affect cyber security of third parties, negative externalities exist. In this situation, their care level is higher than socially optimal and they will overinvest.[21] Moreover, information asymmetries exist for organizations purchasing products to reduce cyber risk, because it is difficult for them to assess the quality of Internet security products.[22] This also leads to underinvestment in care measures, because one is not willing to pay for something of which one cannot verify the quality.[23] Hence, the well-known market failures of positive externalities, negative externalities and information asymmetry avoid the market from reaching the desirable situation.

In the literature, several solutions have been proposed to correct suboptimal care levels caused by externalities and information asymmetries in general. For instance, liability for cyber risks can internalize externalities.[24] Also regulation can affect care levels, for example data breach notification laws which mandate disclosure of data breaches, thereby increasing information about cyber insecurity in the market.[25] Another solution, the central theme in this contribution, is insurance of cyber risks.[26] In as far as insurers have better information about risks than the insured and can induce the insured to take desirable care measures via the insurance contract, insurance can tackle the market failures discussed above. Moreover, the transfer of risks to an insurer results in a reduction of risk, which creates additional social benefits. Section II.C below discusses the benefits of insuring cyber risks more thoroughly. A last solution worth mentioning could be inducing organizations to pool their risks,[27] for

[20] Ross Anderson, Why Information Security is Hard -- An Economic Perspective, Presented at 2001 ACSAC, New Orleans, LA (2001), http://www.acsac.org/2001/papers/110.pdf (accessed 21 March 2016).

[21] Compare for instance the two identical bicycles standing next to each other, one with a outstanding lock and another with a mediocre lock. Suppose a thief has the ability to crack every lock. A thief is likely to steal the bicycle with the smallest lock. Hence, the level of care of the bicycle owner with the outstanding lock has negative externalities for the bicycle owner with the mediocre lock.

[22] Tyler Moore, The Economics of Cybersecurity: Principles and Policy Options, 3 International J. of Critical Infrastructure Protection 3-4, 103-117 (2010).

[23] Anderson, supra note 20.

[24] Faure, supra note 13.

[25] Sasha Romanosky, Rahul Telang & Allesandro Acquisti, Do Data Breach Disclosure Laws Reduce Identity Theft?, 30 J. of Policy Analysis and Management 2, 256-286 (2011).

[26] For insurance in general, see Isaac Ehrlich & Gary S. Becker, Market Insurance, Self-Insurance, and Self-Protection, 80 J. of Political Economy 4, 623-648 (1972). For cyber insurance, see Annette Hofmann & Hidajet Ramaj, Interdependent Risk Networks: The Threat of Cyber Attack, 11 Int. J. of Management and Decision Making 5/6, 312-323 (2011). See also ENISA, and Biener et al., supra note 2.

[27] Michael G. Faure & Ton Hartlief, Insurance and Expanding Systemic Risks, Organisation for Economic Co-operation and Development, online publication 28 June 2003, doi:10.1787/9789264102910-en.

instance through providing financial instruments for risk sharing.[28] Pooling of cyber risks is especially fruitful when risk bearers have more information about the market than insurers, and therefore plays a possible important role in future research towards risk ownership structures in cyber security, as section VI will discuss recommendations.[29]

C. The Potential of Insuring Cyber Risk

As said, this contribution does not aim to thoroughly discuss and compare the various alternatives mentioned above. It focuses on the insurance of cyber risks. The core *raison d'être* of insurance lies in the fact that individuals, and to a lesser extent organizations, are risk averse.[30] Risk averse actors experience a decreasing marginal utility of wealth. This implies that for an identical expected loss, they prefer a larger probability of a smaller loss over a smaller probability of a larger loss. They are even willing to pay more than the expected loss to reduce or remove the uncertainty.[31] The degree of risk aversion is affected by the size of the loss as compared to the size of the assets, and by possibilities of risk diversification. As SMEs are relatively small and have limited ability to effectively diversify, they can be assumed to be risk averse. Hence, firms can use cyber insurance to transfer cyber risks (which are low probability, high impact risks) to the insurer.[32] In as far as firms are more risk averse than insurers, this increases social welfare.[33] Moreover, an additional economic surplus is created when risk is being transferred from the insured to an insurer. The latter has the ability to pool them together with risks of other clients, which due to the 'law of

[28] Goran Skogh, Risk-sharing Institutions for Unpredictable Losses, 155 J. of Theoretical and Institutional Economics 3, 505-515 (1999); Ross Anderson & Tyler Moore, Information Security Economics - and Beyond, Presented at the 2008 9th International Conference on Deontic Logic in Computer Science, Luxembourg (2008), https://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf (accessed 21 March 2016).

[29] Faure & Hartlief, supra note 27.

[30] McKinsey & Company, McKinsey on Finance (2012), http://www.mckinsey.com/client_service/corporate_finance/latest_thinking/~/media/D2CF206B82C34F1FBB87FE591599A958.ashx (accessed 21 March 2016).

[31] See p.377 in Gerhard Wagner, Tort Law and Liability Insurance, in Michael G. Faure, Ed., Tort Law and Economics, Volume I Encyclopedia of Law and Economics, second edition, Cheltenham: Edward Elgar (2009); see p.59 in Peter Zweifel & Roland Eisen, Versicherungsökonomie, Berlin: Springer Verlag (2003); see p.258 in Shavell, supra note 13.

[32] Arunhaba Mukhopadhyay, Samir Chatterjee, Debashis Saha, Ambuj Mahanti & Samir K. Sadhukhan, Cyber-Risk Decision Models: To Insure IT or not?, 56 Decision Support Systems 1, 11-26 (2013); Scott J. Shackelford, Should Your Firm Invest in Cyber Risk Insurance?, 55 Business Horizons 4, 349-356 (2012).

[33] Kesan, Majuca & Yurcik, supra note 1.

the large numbers' reduces risk for the insurer and enables more accurate predictions of the expected losses.[34]

Besides the welfare increasing *transfer* of risk, insurance also stimulates insurers to *reduce* risk by incentivizing desirable behavior of the insured. In as far as insurance companies, being repeat players,[35] have better information about risks and the possibilities to reduce them than their clients, being one-shotters, welfare increases further. By insuring a large number of similar risks, insurers obtain information about these risks, for example the accident probability, the size of the losses, the possible care measures et cetera.[36] This can be done by requiring the insured to take specific care measures, such as installing sprinklers in the field of property insurance, or ensuring up-to-date operating systems and regular security backups in the field of cyber insurance. This increase in the level of care increases social welfare if the costs of investments are lower than their societal benefits. Insurers are more in the position of taking into account social effects because an insurance pool (at least partly) will internalize externalities associated with cyber security. Another way cyber insurers could increase IT safety,[37] is to tie premiums to the insured firm's care level. This creates market-based incentives for organizations to increase their level of IT safety. This kind of expert knowledge of the insurer is also the reason why firms, even if they would not be risk averse, may prefer market insurance over self-insurance.[38]

From the perspective of the insurance company, there are various reasons why offering cyber insurance would be profitable. The demand side of the cyber insurance market mainly consists of firms with a significant amount of IT in their core business process.[39] As a result, insurers have a large number of similar risks available for pooling. Furthermore, cyber insurance differs from more general insurance products and this gives rise to new possibilities for insurers to enlarge their client base, diversify their risk portfolio and to obtain higher profits.

III. CYBER INSURANCE CONTRACTS, PRICES & COMPETITION

[34] George L. Priest, The Current Insurance Crisis and Modern Tort Law, 96 Yale L. J. , 1521-1590 (1987).
[35] Marc Galanter, Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change, 1974 L. and Society 9, 95-160 (1974).
[36] Goran Skogh, Insurance and the Institutional Economics of Financial Intermediation, The Geneva Papers on Risk and Insurance 16, 360-370 (1991).
[37] Kesan et al., supra note 1.
[38] Wagner, supra note 31, p. 379.
[39] Tridib Bandyopadhyay, Vijay S. Mookerjee & Ram C. Rao, Why IT Managers Don't Go for Cyber-Insurance Products, 52 Communication of the ACM 11, 68-73 (2009).

The past section discussed the potential of insuring cyber risk in order to reduce market failures in cyber security. Unfortunately, there are barriers to the utilization of this potential. Both insurance law and economics literature as well as cyber risk literature distinguishes several elements that hinder the insurability of risks.[40] Specific for cyber insurance law (and more broadly for systemic risks) is the fact that insurance contracts have to deal with correlated risks. Also, there are problems of information asymmetry and information unavailability in the context of cyber insurance markets. According to the economic analysis of law, one of the main roles of insurance law is to protect the parties from strategically exploiting hidden information. An information surplus at the side of the insured results in adverse selection (ex ante, before signing the contract) and moral hazard (ex post, after signing the contract).[41] An information surplus at the side of the insurer may result in strategic behavior of the insurer, such as reverse adverse selection.[42]

The current section investigates the hurdles that need to be overcome in cyber insurance contracts, prices and competition in order for cyber insurance to really contribute to social welfare. This section analyzes coverage clauses (section III.A), prices and competitors (B) and adverse selection-, reverse adverse selection and moral hazard measures in subsections C, D, and E respectively. Each subsection considers (i) the socially ideal situation (or main trade-offs that have to be made) and the lessons to be learned from existing insurance literature on cyber risks and systemic risks; (ii) the impediments for growth, how they relate to strategic behavior of the insurer and which contractual solutions insurance companies can use to reach their private optimum and thus diverge from the social optimum; and (iii) the expectations regarding the design of cyber insurance contracts for Dutch SMEs, given these impediments.

[40] See p. 13 in Baruch Berliner, Die Grenzen der Versicherbarkeit von Risiken, Zürich: Schweizerische Rückversicherungsgesellschaft (1982); Faure & Hartlief, supra note 27; Gerhard Wagner, (Un)insurability and the Choice between Market Insurance and Public Compensation Systems, in W.H. van Boom and Michael G. Faure, eds., Shifts in Compensation Between Private and Public Systems, Vienna: Springer Verlag, 87-112 (2007); Wagner, supra note 31.

[41] See among many others, Kenneth J. Arrow, Uncertainty and the Welfare Economics of Medical Care, 53 American Economic Rev., 941-973 (1963); George Akerlof, The Market for Lemons, 84 Quarterly J. of Economics, 488 (1970); Steven Shavell, On Moral Hazard and Insurance, 93 Quarterly J. of Economics, 541-562 (1979); Shavell, supra note 13.

[42] Ex post an information surplus at the insured side can also result in reverse moral hazard, but since this is not observable in the contract itself, this Article will exclude reverse moral hazard from the discussion.

A. Correlated Risks and Coverage

This subsection develops a theoretical framework on coverage for cyber risks under the condition that cyber risks are (at least partly) correlated. Hence this subsection will first discuss the correlated nature of cyber security risks and subsequently the theoretical expectations regarding the impact of correlated risks on coverage clauses.

Risks in an insurance pool need to have some degree of *independence* from each other. Dependent risks, also called correlated risks, have a lower degree of insurability. With correlated risks, the risk of the risk pool does not equal average risk: the law of the large numbers does not work. After all, if a large fraction of all the risks would materialize together, the insurer would not be able to provide coverage for all these simultaneous losses. Thus, correlated risks make the insurance pool inherently instable. Closely connected to the fact that risks should be independent of each other is the fact that an insurable risk should be non-catastrophic, meaning that a single incident should not be so large that it would bankrupt the insurer. Incidents can have a large upside that exceeds the financial reserves of insurers. Capacity problems are especially present when third party damage and secondary damage are covered.[43] A clear example of a catastrophic incident is a nuclear incident.[44]

So-called 'systemic risks' are characterized by the fact that they are not (fully) independent and hence have some degree of correlation. Sometimes they can be even catastrophic. New systemic risks, which result from recent technological advancement, are a specific subset of those risks.[45] Scholars and practitioners regard cyber risk as a new systemic risk.[46] For instance, the CEO of Catlin, Stephen Catlin, warned in February 2015 that cyber risks present the 'biggest, most systemic risk' he has encountered in an insurance career of more than 40 years.[47] The systemic element is caused by the high degree of interdependence of information systems. Existing information technology is designed in a similar way and consequently vulnerable to the same incidents, hence incidents are potentially highly

[43] See for third party damage Howarth Kunreuther, Robin M. Hogarth &Jacqueline Meszaros, Insurer ambiguity and market failure, 7 J. of Risk and Uncertainty 1, 71-87 (1993); see for second party damage Bandyopadhyay, Mookerjee & Rao, supra note 10.

[44] Willem. H. van Boom, Insurance Law and Economics: An Empirical Perspective, in Michael G. Faure & Frank Stephen, eds., Essays in the law and economics of regulation - in honour of Anthony Ogus. Cambridge: Intersentia, pp. 253-276 (2008).

[45] Faure & Hartlief, supra note 27.

[46] Gwen Ackerman, G-20 Urged to Treat Cyber-Attacks as Threat to Economy (2013), http://www.bloomberg.com/news/Articles/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy (accessed 21 March 2016); World Economic Forum, Global Risks 2014, Report for the World Economic Forum (2014).

[47] Gatlin is the owner of the largest syndicate at Lloyd's (Financial Times 5 February 2015).

correlated between firms.[48] When risks are correlated, the expected value of the insurer's pool of risks does not converge to its average; if the risk materializes, many other risks will materialize as well through cascade effects. In theory, there are cyber cases imaginable of perfect correlation, i.e. where all incidents happen at the same point in time: a zero day exploit in a widely used operating system, a large-scale malware attack, or a vulnerability in a widely used operating system. Such cyber incidents can be catastrophic and insurers might not be capable of reimbursing the damage. Nevertheless, there is little empirical evidence about the degree in which cyber risks are correlated. For instance, within 25 years of internet communication, no catastrophic cyber incident, comparable with for instance a big earthquake or the meltdown of a nuclear power plant, has happened so far.

It is difficult to observe which cyber risks affect the continuity and solvency of an insurer. Still, general categorizations can be made, for instance, the distinction between correlated risks and cascade effects. Correlated risks in an insurance portfolio are risks that simultaneously affect several insured parties. Cascade effects occur when the operationalization of one risk as such causes a domino effect at other third parties. A matrix of these types of risks is displayed in Table 1.

- insert Table 1 about here -

In case there are neither cascade effects, nor correlated risks, the risk is in theory independent, and hence perfectly insurable. There are for instance types of coverage that will only operationalize when first party risks are not correlated. An example is reputation damage or, to a lesser extent, the coverage for fines. When only one company is hit by a cyber incident, it is likely that there is potentially significant reputation damage. But when a cyber incident hits many, the reputation damage for each individual company is likely to be small. When a risk does have cascade effects, but is not a correlated risk (one could think of a targeted attack that unleashes third party personal data), third party coverage determines the eventual systemic risk for the insurer. However, caps on claims for these kinds of third party risk are a simple option to mitigate uncorrelated third party risks. With regard to risks that are indeed correlated, the systemic element increases significantly. In that case, as discussed before, risk, for example an exploit that allows for the installment of ransomware, can operationalize simultaneously among several insured in the pool. In that case, the law of the

[48] Walter. S. Baer & Andrew Parkinson, Cyberinsurance in IT Security Management, IEEE Security and Privacy May/June (2007), doi:10.1109/MSP.2007.57 (accessed 21 March 2016).

large numbers is not applicable anymore. Potential cascade effects increase the impact of correlated risks even further. Thus: "correlated risks are not so much an impediment to efficiency but a category of risks that are generally hard to insure".[49]

What are the implications of the systemic element of cyber risks for the optimal design of cyber insurance coverage from a social welfare perspective? The question is whether the category of cyber risks that SMEs want to insure overlaps with the category of cyber risks that insurers are willing to insure, given the aforementioned systemic uncertainties. Arguably, social welfare could be increased when SMEs can transfer cyber risks they cannot bear (i.e. low probability - high impact risks) to an insurer that can bear them and is willing to bear them. This also implies that, from a rational actor perspective, SMEs do not insure cyber risks that they can bear (low impact risks). Although the perception of 'high impact' might vary across the size, organizational type and risk appetite of SMEs, in general it would be desirable for them to have relatively high deductibles and high caps. However, insurers should manage the risk of large-scale cyber incidents and may therefore demand lower caps to reduce the risk of a 'catastrophic upside' due to cascade effects. These two conflicting interests should be traded off to reach a final outcome.[50]

The exact types of coverage to be included are closely related to the insurance premium and the cap. On the one hand, more limited coverage leads to lower premiums but also implies that the insured will not receive compensation for costs resulting from excluded events. For SMEs, it depends on the type of company which costs are most urgent to cover. For companies with many third party personal data, for instance, potential costs related to third party damage could be the highest and therefore most urgent to cover, especially due to possible cascade effects of a cyber incident. These costs include claims, fines, legal expenses, and crisis control expenses in case of lost of client and/or company information. On the other hand, for the insured, insured risks that have a high likelihood of being correlated might be difficult to insure because of their negative impact on the distribution of the insurance pool.

Would it be desirable that insurance companies offer the same coverage? A clear advantage is the comparability of policies across insurers, facilitating transparent decision making for firms looking for insurance. Besides, loss data can be aggregated straightforwardly which might help to solve the broader problem of information unavailability, which will be discussed in section III.B. On the other hand, fixed contracts do

[49] Ronen Avraham, The Economics of Insurance Law - A Primer, 19 Conn. Ins. L.J. 29-112 (2012).

[50] Another regulatory option to overcome the risk of insolvency of insurers is governmental insurance or governmental bailout for cyber risks with a catastrophic upside.

not allow insurers to differentiate their products and might hinder the development of a free and open market. The fast changing nature of cyber products and the specific character of cyber threats, being different for each type of company, are also important argument for tailor-made insurance contracts. Recent US cases point out that it is important that cyber insurance contracts contain very precise coverage clauses in order to ensure legal security and prevent interpretation arguments. [51] At the same time, extensive formulations and exclusions could restrict the applicability of the insurance clauses, especially in the light of the fast changing nature of cyber risks.

Within cyber insurance, the extent to which an insurer accepts the transfer of risks depends on its own risk preference and on its ability to effectively mitigate and disentangle the correlation between various cyber risks. Insurers can take measures to reduce the correlated character of risks, by, among others, getting more customers and diversify among operating systems, sectors and countries.[52] So, which risks should a cyber insurer include, and which risk should a cyber insurer exclude? In a social optimal situation, insurers solely exclude cyber risks that have a high likelihood of affecting their solvency and liquidity. It could be that, due to the lack of data, insurers could have false impressions that certain cyber risks are strongly correlated and may severely impact solvency and liquidity, while they in fact are bearable. In that sense, social gains can mostly be realized if insurers exclude risks that they in fact can bear.. For instance, when insurers indeed have few customers, how likely is it that correlated risks indeed affect their solvency ratio's, which might justify low caps? It is important to note in this respect that this research focuses on the analysis of cyber insurance contracts. Hence this set-up cannot observe the insurance pool, apart from anecdotal evidence about the number of clients that insurers indicate themselves. This implies that this research cannot observe the insurers efforts to reduce the correlated character of its risk by diversification. The research setup can, however, implicitly observe the insurers efforts to enlarge its pool and thus diversify, by observing the attractiveness of its insurance products to potential customers.

In the field of cyber security risks, with limited information about risks forecasts and the degree of correlation, one might expect that risk averse insurers would prefer the

[51] *Travelers Indemnity Co. of America* v. *Portal Healthcare Solutions LLC*, case number 14-1944, in the U.S. Court of Appeals for the Fourth Circuit; Recall *Total Information Management Inc. et al.* v. *Federal Insurance Co. et al.*, case number SC19291, in the Connecticut Supreme Court.

[52] Although the Internet is borderless, its diversification among countries would probably still reduce the correlation between risks as for instance some sorts of cybercrime tend to be targeted at specific countries or subsets of industries.

likelihood of covering too little (and gain less market share) over the likelihood of covering too much (and ultimately risk insolvency). Hence, the expectation is that the contracts offered in the market still deviate from the social optimum. This means that they would have (i) relatively low caps on payable sums, in the sense that for the insured there is still a significant residual uninsured risk; and (ii) exclusion clauses of catastrophic and/or correlated risks, as well as exclusions for risks that are reasonably believed to be non-catastrophic or not extremely correlated, incented by the aforementioned private optimum of the insurer.

B. Prices and Competitors

Besides looking at cyber insurance contracts, as a side effect, this case study also has the possibility to observe prices and the number of competitors in the market. This section discusses what currently is known about the prices and competitors in the market in order to formulate expectations about the market. Subsequently, we argue that the nature of cyber risks has a large influence on prices and competition.

In the US cyber insurance market, the annual gross premiums written are an estimated 1.3 billion USD and growing 10-25% yearly,[53] and 32% in 2014.[54] Simultaneously, the premiums in the US are going down from 4.5-5% of the amount covered in 1999 and 1-2.5% in 2000 to 0.50-6.00% in 2004.[55] Estimates of the fraction of US firms that has purchased cyber insurance in 2013 vary between 6 and 19%.[56] There are huge differences between sectors, running from 1-2% of firms in the manufacturing and health sector to 20% in the financial sector.[57]

Although exact sales figures vary, the European market for cyber insurances has evolved over the past ten years, possibly driven by the implementation of further reaching

[53] Richard S. Betterley, Cyber/Privacy Insurance Market Survey 2013, The Betterley Report (2013), http://betterley.com/samples/cpims13_nt.pdf (accessed 21 March 2016).

[54] Peter J. Beshar, Protecting America from Cyber-Attacks: The Importance of Information Sharing, US Senate Committee on Homeland Security & Governmental Affairs, hearing U.S. Senate Committee on Homeland Security (2015), http://www.hsgac.senate.gov/hearings/protecting-america-from-cyber-attacks-the-importance-of-information-sharing (accessed 21 March 2016).

[55] Luzwick, and Kesan et al., supra note 1.

[56] Willis (2013) estimates that 6-10% of the US firms purchased cyber insurance whereas the Harvard Business Review (2013) reports that 19% has done so. Willis, Willis Fortune 1000 Cyber Disclosure Report (2013), http://blog.willis.com/downloads/cyber-disclosure-fortune-1000/ (accessed 21 March 2016); Harvard Business Review, Meeting the cyber risk challenge (2012), http://www.computerweekly.com/blogs/public-sector/Meeting%20the%20Cyber%20Risk%20Challenge%20-%20Harvard%20Business%20Review%20-%20Zurich%20Insurance%20group.pdf, (accessed 21 March 2016).

[57] Willis, supra note 56.

data breach notification laws.[58] Especially financial institutions regard cyber risk as a very important risk to deal with.[59] In 2013, approximately 10% of European firms was actually insured.[60] The annual gross premiums written equal 192 million USD in 2013 and are expected to reach 1.1 billion USD in 2018.[61]

For the Netherlands, no sales figures are available. The Dutch Association of Insurers concludes that cyber risks are by far not as insured as in the US,[62] even though, according to the association, cyber-crime in the Netherlands is estimated to cause at least 13 billion USD in losses, possibly even two or three times as much.[63] However, there are also scientific studies that stress the systematic overstatement of the cost of cybercrime.[64] 'Anecdotal evidence' indeed suggests that cyber insurance is not widely used in the Netherlands, especially when it concerns SMEs. Hiscox only encountered two claims for their DataRisk policy in their first two years of service.[65] An underwriter of Chubb Specialty Insurance interviewed in August 2015 indicates off the record that annually ten policies are sold. An HDI-Gerling underwriter observes that firms are interested in cyber insurance but that few policies are actually sold. We co-designed a survey among owners SMEs that did undergo an ethical hack.[66] This survey revealed that Dutch SMEs have little interest in cyber insurance. Only 11% of the respondents indicated to consider purchasing cyber insurance, just minutes after their systems were hacked by hackers with their consent. A sales agent of Zurich that was interviewed, off the record, for this research stated that the costs of cyber insurance

[58] ENISA, supra note 2.

[59] Judy Greenwald, Financial institutions identify cyber risk as major concern: Survey, Business Insurance 2014 http://www.businessinsurance.com/Article/20141023/NEWS07/141029882, (accessed 21 March 2016).

[60] Marsh, 2013 Cyber Risk Survey Marsh Ltd. (2013), https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20Survey%2006-2013.pdf (accessed 21 March 2016).

[61] NAIC, Cyber Risk (2013), http://www.naic.org/cipr_topics/topic_cyber_risk.htm,(accessed 21 March 2016).

[62] Verbond van Verzekeraars, Virtuele risico's, echte schade, Hiscox Netherlands (2013), http://www.hiscox.nl/sites/www.hiscoxnl.com/files/filedepot/cyber-risks-informatie.pdf.pdf (accessed 21 March 2016).

[63] Van de Laar, supra note 1.

[64] Markus Riek, Rainer Böhme, Michael Ciere, Carlos Ganan & Michel van Eeten, Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries, Working paper TU Delft (2016).

[65] Id .

[66] Dutch Network Group, Grip op Cybercrime in Ondernemend Nederland (2016) http://www.dutchnetworkgroup.com/2878/grip-cybercrime-ondernemend-nederland.htm , (accessed 20 September 2016). The Authors co-designed this survey together with the Dutch association for SMEs (MKB Nederland).

outweigh the benefits for small and medium companies. Also literature suggests that premiums are too high for SMEs.[67]

Currently, according to scholars in the market, a lack of *actuarial data*[68] about cyber incidents makes it impossible for insurers to accurately calculate cyber risk and loss potential.[69] Given the relative youth of the Internet and cyber insurance, there is simply only limited actuarial historical data available. Moreover, incidents are scarce or major devastating incidents did not even happen.[70] The lack of good quality actuarial data about cyber incidents hinders forecasts.[71] In addition, there is also a risk of change, in the sense that the cyber security landscape and its risks can change very rapidly and past data loses its value quickly to accurately forecast future risks.[72] Moreover, as discussed in section II.A, cyber risks are correlated risks, which means that incidents do not always emerge independent of each other. Lack of data, the risk of change and the correlated character of cyber risks causes uncertainty about the distribution of risks in the future, which is of paramount importance in determining prices for insurance products. In the end, the lack of accurate cyber risk data and trustworthy future risk determination is widely discussed as the root cause for the slow development of the cyber insurance market.[73]

The question remains how insurers will respond pricewise to systemic uncertainties and what is a preferable reaction from a social welfare perspective. We sketch two scenarios. In the first scenario, insurers react to this uncertainty by increasing their premiums to reflect the uncertainty. Law and economics literature labels this 'insurer ambiguity'.[74] Insurer ambiguity follows the assumption that in situations where there is less insurability, insurers will increase the premium to incorporate the additional uncertainty.[75] Insurer ambiguity will most likely result in a 'Catch-22': insurers need a frequently refreshed dashboard of actual claim data in order to deliver affordable insurance policies, but this data will not be available as long as insurers cannot offer affordable insurance policies. In such a scenario, competition

[67] Biener et al., supra note 2.

[68] Existing data breach notification data does not solve this problem: it is solely systematically recorded in the United States, but this dataset is incomplete because not all notifications are recorded and companies have an incentive to conceal data breaches. In addition, data breach is only a fraction of insurable risk.

[69] William Yurcik & David Doss, CyberInsurance: A Market Solution to the Internet Security Market Failure, Paper presented at 1st 2002 Workshop on the Economics of Information Security (WEIS), Berkeley, CA (2002).

[70] Id .

[71] Id .

[72] Tajalizadehkhoob et al., supra note 14.

[73] ENISA, and Biener et al., supra note 2.

[74] Kunreuther et al., supra note 43.

[75] Prices can also be high because of insufficient competition. Avraham mentions capital requirements, unfair competition or regulatory standards. See note 49.

would develop likewise very slowly. Due to the lack of data, the fact that the pooling opportunities in a small market are limited,[76] and the correlated risks in cyber security,[77] we expect that, in this scenario, only few insurers offering cyber insurance.[78] Limited competition and the aforementioned insurer ambiguity in turn can result in high prices, as the market possibly is not competitive enough when the number of suppliers is low.

In the second scenario, insurers primarily react to the opportunities the emerging new cyber insurance market bring in the sense that new products can be developed, new insurances can be signed and more revenue can be made. In this scenario, insurers will penetrate the market aggressively by a low price/coverage ratio to gain market share despite risk of systemic uncertainties.[79] Fierce competition will break through the 'Catch-22', since in the struggle of gaining market share, insurers will attract customers and hence claim data, which will lower information unavailability and uncertainty. Because most traditional insurances focus on high impact/low likelihood risks, they are often are able to build products with very attractive premiums with respect to the downside that is covered. For instance, as an illustration, premiums for *liability* insurance for SMEs can be €150.04 per year, and 0.003% of the insured amount.[80] Although aggressive pricing strategies in a very competitive market can help to lower prices, such low prices can only be achieved if cyber insurance covers only high (on a company level, maybe even catastrophic) impact, low likelihood risks, following from the discussion in III.A.

Hence, the second scenario is preferable from a social welfare perspective, because in such as situation welfare enhancing risk transfer and subsequently risk reduction measures can be taken. In such a situation we expect primarily large and diversified insurance companies entering the market, because they can afford to take potential losses when penetrating the market.

The expectations regarding prices and competition can be summarized as follows, depending on the strategy followed by insurers: (i) pricing models do not function well as there is only limited data and there is much uncertainty about the exact risks involved.[81]

---

[76] Yurcik & Doss, supra note 71.

[77] Hulisi Öğüt, Srinivasan Raghunathan, and Nirup M. Menon, Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection, 31 RISK ANALYSIS 3, 497-512 (2011).

[78] Van de Laar, supra note 1.

[79] And taking relatively few adverse selection measures to increase the insurance pool even further.

[80] An 'MKB Meerkeuzepolis' of Achmea in 2015 with an insurable amount of 5 million euro. Details available upon request.

[81] Shackelford, supra note 32; Betterley, supra note 53.

Insurer ambiguity therefore causes relatively high premiums and limited competition;[82] and (ii) insurance companies entering the market want to gain market share and hence offer relatively low prices. Competition is mainly amongst large and diversified insurance companies.

C. Adverse Selection

For insurance in general, and for cyber insurance specifically, adverse selection is an impediment for market development.[83] Adverse selection results from the information advantage of the insured that he strategically can exploit before the contract is signed.[84] Adverse selection is caused by the fact that the insurer does not have full information about the characteristics of the insured that determine its risk, before the contract is signed.[85] [86] Therefore (some) characteristics of the insurer, important for risk determination, remain undisclosed. This does not mean that an insurer cannot make a risk profile at all. Regarding cyber risks for instance, the sector in general might be an indicator of increased risk. One might regard online gambling and adult industries as high risk industries, but also law firms that deal with personally sensitive data. But in most cases, an insurer with increased cyber risk is not so easy to detect. Detecting vulnerabilities and potential exploits might be time-consuming, technically complicated, and hence costly. Therefore, it is impossible to calculate an insurance premium that is perfectly fine-tuned to risks specifically for the individual insured.

Adverse selection has important consequences for the insurance pool. As an effect of the inability to tie premiums to individual risk profiles, the premium is based on the average risk distribution in the pool. Consequently, low risk insured firms, which may have better information themselves about their own risk, might find this average premium too high for their individual expected risk and as a result drop out of the pool. Simultaneously, firms with a risk above average are more likely to buy cyber insurance. For example, firms that have experienced cyber incidents will probably be more willing to buy cyber insurance, and if these incidents where due to a suboptimal state of security, this increases the average risk in

[82] Biener et al., supra note 2.
[83] Böhme & Schwartz, supra note 2.
[84] For cyber risks specifically, it is doubtful whether the information advantage of the insured towards the insurer really is that large. Will ex ante high risk SMEs indeed know that they have outdated computer systems, or that they behave more carelessly? This question is still unanswered in the literature.
[85] Akerlof, supra note 41 ; p.320ff in Zweifel and Eisen, supra note 31.
[86] Böhme & Schwartz assume this in their cyber insurance framework. See note 2.

the pool.[87] An increase of average risk in the pool might force the insurer to increase premiums, after which firms with relatively low risks that were left might decide to leave the pool, which increases the risk in the pool even further, et cetera. Due to this adverse selection, low risk actors might not be able to buy insurance coverage against a fair premium (based on their expected risk), which reduces social welfare.[88]

There are various contractual solutions that mitigate the effect of adverse selection in cyber insurance. We discuss the desirability of exclusion clauses, application forms and deductibles.[89] In general, the intensity of measures to reduce adverse selection negatively affects the size of the insurance pool. This will reduce the ability of insurers to gather enough data and accurately estimate risk distribution in the pool. The trade-off between reducing adverse selection and improving data is similar to what the discussion in section III.A on coverage and prices. The adverse selection measures aimed at aligning risks in the insurance pool has the costs of leaving insurance pools small and hence retrieving less data which is needed for a mature cyber insurance market. Hence, severe exclusion or measures to select low risk insured firms in the pool may limit the amount of data that will be collected and might not be desirable in a socially optimal situation.

From the various contractual solutions that mitigate adverse selection, exclusion clauses are probably the most uncomplicated. Exclusion clauses simply exclude certain categories of insured from having a particular form of insurance because they (are perceived to) have an above average risk. Because of their simplicity and conventionality, we expect insurers to include exclusion clauses for general types of business, especially for companies with a high risk profile such as online gambling and adult industry.

A more sophisticated way of exclusion is to exclude certain types of behavior. These are exclusions in case the insured does not fulfill the requirements set by the insurer concerning protection and updating standards. In practice, insurers in the past rarely differentiated premiums depending on the security practices of their clients.[90]

Incorporating too many exclusion clauses in the contract has a negative social effect, as it might exclude high risk insureds. When high risk insureds are excluded from a risk pool,

[87] Shackelford, supra note 32.

[88] However, this problem is partly mitigated through propitious selection: the fact that low risk actors might be more risk averse and high risk actors are more risk prone, and hence they both opt for the same pool which will stay intact.

[89] This means this Article leaves many other adverse selection measures out of the scope of this discussion, for instance, cream skimming, offering insurance products through agencies, aggravation of the severity of risk by the insurer in order to attract risk averse entities, ex post identification of adverse selection.

[90] ENISA, supra note 2.

the insurer has no incentive to reduce these risks, while this might be just the types of entities at which risk reduction is most welfare enhancing since there is many potential for improvement. Moreover, uninsured high risk insureds can negatively affect the risk of insured low risk insurers due to correlations of risk. Internalization of this risk by including these entities in the risk pool on the other hand internalizes these externalities gives extra incentives for the insurer to reduce risk in the pool.

Nevertheless, in a social optimum some actions should be taken by insurance companies to limit adverse selection problems. One way to tackle these problems is by identifying firm's risk characteristics through application forms. Not to exclude them but, to a certain extent, to tie premiums to the perceived risk profile. It is questionable how trustworthy and necessary very extensive application forms are, as one might argue that many SMEs do not have sufficient knowledge about their cyber risks themselves and might be overoptimistic regarding their cyber secure situation. Furthermore, extensive forms limit easy access to insurance products, which slows market growth. Concluding: in an ideal situation forms may be short and just require basic questions, such as the number of employees, turnover and sector.

The height of the deductible is an also an implicit way to identify and exclude high risk or risk averse entities. Different deductibles can have a signaling function of the perception of risk attitude.[91] Section III.A suggested that high deductibles may be beneficial for the development of the market because premiums can be low and a relatively large upside can be covered. When one wants to focus on the insurance pool growth, however, low deductibles are preferred because high deductibles are believed to implicitly exclude high risk entities. Hence, there is a trade-off between coverage, prices and deductibles. Section III.E provides an additional discussion about deductibles in the context of moral hazard.

From the perspective of the insurance company, risk classification is a desirable way to reduce adverse selection problems. Through an identification of risk before the contract is written, different firms can be placed in different risk pools with corresponding premiums and coverage clauses. This differentiation avoids cross-subsidization of low-risk entities towards high-risk entities, as well as too large discrepancies between the expected risk of individual firms and the average risk in the pool.[92]

Again, the expectations about which adverse selection measures in the policies would lead to a private optimum for the insurance companies are two-fold, and depend on the

[91] Avraham, supra note 49.
[92] Priest, supra note 34.

insurers' risk profile. A risk prone insurer strives for enough market share and chooses to reduce adverse selection measures. In this private optimum, the insurance company will probably offer easy requesting procedures and low deductibles and exclude little to none risk categories. A risk averse insurer is probably much more concerned with the correlated nature of cyber risks, and is eager to know a lot about potential clients through extensive cyber security audits before the contract is written.[93] Here an auditing agency performs an extensive and costly inspection of the security behavior of an organization. The agency informs the insurer, who in turn designs the contract tailored to the firm specifics. Another possibility for risk averse insurers to acquire information is via the requesting procedure. For this type of insurance companies, we expect a complicated and extensive requesting procedure.

Ultimately, more risk prone insurers will contribute to social welfare because they will generate more clients which enables a better risk pool and more subsequently more claim data which enables better insights on how to reduce risk. The main trade-off for those risk prone insurers is to choose between high or low deductibles in relation with market share and price. From a social welfare perspective, high deductibles would be preferable to low deductibles. High deductibles reduce adverse selection and moral hazard, move the insurance products more in a low likelihood high impact category and enable the insurer to offer lower prices.

D. Reverse Adverse Selection

Although there is little data available about the cyber insurance market,[94] insurers do have more information about incidents than their customers. Insurers have data of the combined claims of their customers, and they can put more resources in understanding the value of each coverage clause than potential insured can. This information asymmetry could elicit strategic behavior of the insurance companies: they could strategically impose barriers for consumers to assess premiums on high or low quality. Also they can deliberately exaggerate cyber security risk as a marketing strategy to make it harder for consumers to make an informed choice and assess which types of coverage they really need.[95] When there is an information surplus at the side of the insurers and it is costly for potential insured firms to acquire this

[93] Anderson & Moore, supra note 28.
[94] ENISA, supra note 2.
[95] Riek et al., supra note 64.

information, insurers can use this advantage to reduce adverse selection. Eventually, insurance companies could use their information surplus to reversely adversely select their customers, [96] and actively sustain the 'market for lemons' in the sense that insurers present their coverage clauses in a way that is difficult to understand for SMEs, not being cyber experts. In the long run, this behavior would lead to a race to the bottom with low quality insurance products.

Although the previous scenario might lead to a private optimum for insurance companies, reverse adverse selection should be cancelled out to reach a social optimum. Transparency in the applicability and limits of the insurance contracts is the key concept in counteracting reverse adverse selection.[97] This way, relatively uninformed firms looking for cyber insurance are also able to make an informed choice and understand the value of the coverage. Recent case law in the United States regarding cyber insurance underlines the importance of policies with clear and appropriate (cyber-specific) language and unambiguous coverage boundaries.[98] Fixed contracts, with fixed coverage clauses, can aid in reducing reverse adverse selection. However, as is discussed in section III.A, tailor made contracts allow for more flexibility that might be needed in the fast changing nature of the internet.

E. Moral Hazard

Moral hazard occurs after the insurance contract is closed.[99] The insured might start behaving differently (i.e. take less care) because he does not bear the losses of a damaging event himself anymore.[100] It is too costly for the insurer to perfectly monitor the behavior of the insured, which can therefore exhibit these hidden actions. This influences the expected losses, so that the insurance premium has to rise. Regarding the problem of moral hazard, three types are relevant for the cyber insurance market.[101] First, the insured party can take fewer precautions against the insured risk, leading to ex-ante moral hazard. Second, the

---

[96] Avraham p. 32, supra note 49.

[97] Id.

[98] *Travelers Indemnity Co. of America* v. *Portal Healthcare Solutions LLC*, case number 14-1944, in the U.S. Court of Appeals for the Fourth Circuit*; Travelers Property Casualty Company of America et al.* v. *Federal Recovery Services et al.*, case number 2:14-cv-00170, in the U.S. District Court for the District of Utah.

[99] Moral hazard is closely linked to adverse selection, in the sense that high risk entities ex ante have more impact when they exert moral hazard. Moreover, it is often hard to distinguish moral hazard from adverse selection empirically.

[100] Shavell, supra note 41; Shavell, supra note 13.

[101] Liam M. D. Bailey, Mitigating Moral Hazard in Cyber-Risk Insurance, 3 J. of L. & Cyber Warfare 1, 1-44 (2014).

insured may take insufficient measures to mitigate potential losses in the event of an insured occurrence: ex-post moral hazard. Third, an insured party could increase losses in order to secure larger reimbursements under an insurance contract, which essentially is fraud. The situation of network security interdependence that is distinctive for cyber security, magnifies the moral hazard effect as everyone is interlinked.[102] In case insurers are not able to distinguish between insured companies that take proper care measures and companies that do not, insurers charge higher premiums to all insured firms,[103] which again may trigger adverse selection and low risk insurers to drop out of the pool.

This section focuses on requirements in contracts aiming to mitigate the first two types of moral hazard. The main social welfare enhancement is realized by the fact that insurers can transfer information about cyber security to the insured. For instance, the insurer may require the insured to take specific care measures, and decline or lower payout in case the care measures are not implemented or not taken sufficiently. Another socially desirable moral hazard measure is information sharing among insurance companies.[104] When they anonymously share information as historical loss data, claim histories, and compliance audits through an independent, government funded information sharing platform, individual premiums can be adjusted contingent on a corresponding investment in information security infrastructure. Accordingly, insurers reduce their own risk of loss and create economic incentive for insured to adequately secure consumer information. Besides, the existence of such an information sharing network lowers the entry costs of the cyber insurance market for interested insurance companies. Additional insurers can compete with current market participants creating a more competitive market place, leading to increase in risk adjustment and underwriting protocols, and increasingly affordable cyber insurance policies.[105]

We expect individual insurance companies to impose measures in their contracts to counteract moral hazard incented behavior of the insured, including partial coverage, caps on payable sums, co-insurance and deductibles.[106] Moreover, insurance companies most likely

---

[102] Nikhil Shetty, Galina Schwartz, Mark Felegyhazi & Jean Walrand, Competitive Cyber-Insurance and Internet Security, in T. Moore, D. Pym, and C. Ioannidis, eds., Economics of Information Security and Orivacy, New York: Springer, pp. 229-247 (2010).

[103] Avraham, supra note 49.

[104] Bailey, supra note 103.

[105] Despite the theoretical value of this approach towards information sharing, the practical value seems to be limited from a practical point of view: early market participants are in this set-up asked to share their data (which they have gathered in an undeveloped and possibly risky insurance market) with other insurers such that these can take position in the market and compete with sharp prices. Nevertheless, insurance companies do not appear to be willing to share data as these figures are part of their core business.

[106] Shavell, supra note 41; Shavell, supra note 13; Wagner, supra note 31.

require certain care measures from their clients, and that careless behavior from the side of the insured will lead to (partly) exclusion from payment. In order to combat ex-post moral hazard, we expect insurance clauses that partially expose the insured party to risk,[107] via caps on payable sums and deductibles for the same reason. In order to mitigate ex-ante moral hazard, we expect that the insurer differentiates premiums based on the security practices of the insured party,[108] and based on feature and experienced risk rating methodologies.[109] Further fine-tuning of the premium could be reached via bonus/malus arrangements or no-claim discounts.

IV. Empirical Strategy

This case study selected cyber insurance contracts for SMEs to compare actual offers to theoretical framework. Moreover, the focus lays on the Dutch market. The Netherlands is an example of a European country with a well-developed digital infrastructure and it is connected to other EU Member States through the EU internal market. Insurers that offer cyber insurance in the Netherlands are large international insurance companies. Thus, results might differ quantitatively across countries in the EU, but qualitatively, the conclusions can be generalized to other countries in the EU and/or with a highly developed digital economy, such as the US. The focus lies on SMEs because they are an important part of the Dutch society. About 99% of the Dutch companies are SMEs and SMEs have a share of 60% in Dutch GDP.[110] Moreover, SMEs are vulnerable for cyber-attacks while, because of their size, specified protection products may be produced insufficiently and SMEs themselves lack understanding of cyber security risks.[111] Also, because of the interrelatedness of cyber security risks, improving the 'weakest links' potentially also benefits better protected large companies, for instance when SMEs function as a back door to infiltrate larger companies.

---

[107] Faure & Hartlief, supra note 27 .

[108] Shetty et al., supra note 104.

[109] Bailey, supra note 103.

[110] Jan De Kok, Yvonne Prince & Tommy Span, De bijdrage van het MKB aan de Nederlandse economie, Zoetermeer: Panteia (2015).

[111] PGI Cyber, SMEs are Vulnerable to Cyber Attacks (August 2015), https://pgicyber.com/NewsandEvents/SMEs-are-vulnerable-to-Cyber-Attacks (visited September 20, 2016); Jessica Fino, Vast Majority of SMEs Vulnerable to Cyber Attacks and IT Threats, Survey Finds (July 2016) http://economia.icaew.com/news/july-2016/smes-vulnerable-to-cyber-attacks-and-it-threats (visited September 20, 2016).

The authors requested cyber insurance contracts on behalf of six firms. Three firms are currently operating in the Netherlands and three organizations are artificially constructed:[112]

- **Arbinn** is a small consultancy company for the energy- & utility sector
- **Banketbakkerij de Waal** (artificially constructed) is a Dutch local bakery
- **Desiderius** (artificially constructed) is a tax advice company for Dutch SMEs
- **Eigensteil** is a full-service Internet company, focusing on graphic design and software development
- **FaceXXX** (artificially constructed) is a Dutch adult industry website
- **Unibarge** is a logistic operator in the Rotterdam harbor

The firms vary in size and dependency on IT infrastructure, in order to analyze whether insurers differentiate their offers. Eigensteil and Desiderius are the only two firms with a turnover of higher than 1 million euros. Banketbakkerij de Waal has a low Internet dependency, Unibarge, Arbinn and Desiderius have a medium Internet dependency and FaceXXX and Eigensteil have a high Internet dependency.

For each of these companies, the Authors requested insurance offers from nine insurers offering cyber insurance to European SMEs: ACE, AIG, Allianz, AON, CNA, Chubb, Hiscox, HDI-Gerling and XL. HDI-Gerling only offered a policy focusing on Internet banking fraud at the time of the empirical observation. To the best of the Authors knowledge all insurance companies operating on the Dutch market are approached.

The overview of typical cyber insurance policies in Biener et al. (2015) is the starting point for the analysis of coverage clauses.[113] This framework scores policies on types of coverage (e.g. network security liability and business interruption), causes of cyber loss (e.g. hacking and insertion of computer viruses), and insured losses (e.g. loss of profit and legal liabilities). In addition, the Authors documented policy exclusions and conditions that deviate from those in other policies.

For purposes of comparison, similar amounts for coverage, deductibles and caps were requested. In case of standardized policies with limited choice, this was not possible. The insurance application process was registered as well.

V. RESULTS AND DISCUSSION

[112] An extensive description of the organizations is available upon request.
[113] Biener et al., supra note 2.

This section presents the main findings of the case study. The presentation of results and discussion follows the chronological process of the purchase of cyber insurance. First, the requesting procedure is discused, followed by the price of the product and subsequently coverage, caps & deductibles and risk reduction measures. The discussion is ended with a more high level synthesis of insurers and their strategies.

A. Requesting Procedure

AON and Hiscox do not check a cyber insurance request ex ante and enable signing an online contract immediately. AIG and Chubb require filling out a 7- or 11-page request form with questions concerning information security policies, personnel hiring practices, premises -, web server -, and mobile device security, service providers, PCI -, and HIPAA compliance,[114] written records management, and data breach incident response. The other insurance companies gather information through their brokers, which require more detailed information. In 80% of the cases it was difficult and time consuming to request insurance offers from the insurer, which is illustrated by the fact that it took the Authors four months to get an overview of the available offers in the market.

On forehand, insurers do not exclude firms as such from cyber insurance. They rather exclude certain damages, claims and other losses that follow from specific activities. Three of the policies the Authors received contain adverse selection clauses. Allianz, Hiscox, and LIU exclude gambling activities. In addition, Allianz excludes adult businesses as well. AON and Chubb do not have adverse selection clauses, but state explicitly in their cyber product brochures that they are cautious of credit card companies, data aggregators and warehouses, payroll processing, gaming and social networks (Chubb) and firms active in the field of gambling, jackpots and porn (AON). Consequently, firms operating in these businesses may not be interested in insurance from these insurers. None of the insurances extensively evaluated the security practices with an in-house assessment; insurers apparently are convinced that request forms provide sufficient information to offer coverage.

With regard to ex ante requesting cyber insurance, we observe two elements. First, we observe both easy to fill in, as well as complicated and extensive requesting procedures, which would indicate that indeed insurers are either following the strategy of gaining quick market share or rigorous risk control. However, a differentiation of premiums based on the

[114] PCI: Payment Card Industry Data Security Standard; HIPAA: Health Insurance Portability and Accountability Act.

estimated ex ante cyber risk of the insured is not observed. In other words, there are currently no adverse selection measures apart from the exclusions mentioned and differences in the choice of deductibles. This is especially interesting because as mentioned, some insurers indeed requested much information about the state of security of their potential clients, but are not using it.

B. Premiums

The results show that premiums for firms with a turnover below 1 million are 0.26-0.53% of the insured amounts. For companies with a turnover above 1 million, they are 0.32-0.99%. Thus, premiums vary between 0.26% and 0.99% of the insured amount. Table 2 presents an overview. Figure 1 shows a clustering of premiums between 0.30% and 0.40%. Premiums in the Dutch market in 2015 hence are two times lower than the US amounts in 2004 on the low end, and six times as low on the high end. The average annual premium for small companies for €250,000 coverage is €1,000, which does not seem insurmountable. Still, as an illustration, premiums for *liability* insurance for small companies are much lower, e.g. €150.04 per year, with a coverage of €2,000,000.[115] This, of course, does not imply that cyber insurance is too expensive, because for such an evaluation one needs to know the loss ratios (losses of accepted claims divided by premiums). Unfortunately, besides anecdotal 'off the record' evidence, there is no information on these loss ratios.[116]

- insert Table 2 about here-

None of the contracts contained any clauses concerning some bonus/malus system in which no-claim behavior is rewarded with lower premiums and vice versa. The small differences between premiums offered for different turnovers also indicate that insurers are not interested in behavior-based premium differentiation or that they simply do not have the right data and tools to do so.

[115] An 'MKB Meerkeuzepolis' of Achmea in 2015 with an insurable amount of 5 million euro. Details available upon request.

[116] The Authors asked insurers for the loss ratio and received off the record indications of a loss ratio of 10%, which might indicate that the premium is indeed too high as compared to the exposures to loss.

C. Coverage

We scored the various policies according to the framework of elements in 'typical cyber insurance policies' designed by Biener et al.[117] There are six different complete coverage clauses of seven insurers for observation. AIG and AON use the same policy, XL did not provide a policy and HDI-Gerling solely offers Internet banking insurance. The first three columns of Table 3 present a brief description of the insurable elements. The last column indicates how many insurers out of seven provide coverage for each type. [118]

- insert Table 3 about here -

All insurers in principle cover first party damage and third party liabilities, however they differ in the specific coverage limits and causes: there is variation in coverage for losses caused by employees, systems or third parties. These distinctions might be explained by the insurer's desire to discourage careless behavior of the insured. Business interruption because of non-usable ICT services for example, is not covered by Hiscox and Allianz in case the interruption is caused by activities of the insured or security errors. Despite this exclusion, there are no indications that the premiums of these two insurers are lower than those of other insurers. Allianz and Chubb both cover loss of income due to business interruption. However, Allianz only covers this when caused by a third party, whereas Chubb also covers it when caused by the insured or a security error.[119] This 'devil in the details' matters for instance when one considers insurance for damage resulting from outsourced IT activities. Solely two out of seven insurers cover this vicarious liability, while many SMEs outsource IT activities.

The coverage for losses and expenses following from the insured activities varies a lot across insurers. For example, both HDI-Gerling and Chubb provide first-party coverage for loss of personal data caused by the insurer. HDI-Gerling covers expenses for forensic investigation, PR-advice, legal advice and privacy notification. Chubb covers the same expenses, but also an incident response team, temporary capacity, credit control and digital asset replacement. Crisis control and legal liability, in the context of privacy violation, are covered by all insurers, but the coverage width differs strongly across the insurers. For example, two of them (ACE and Chubb) explicitly exclude the insurance of regulatory fines,

[117] Biener et al., supra note 2.
[118] The detailed comparison is displayed in Table A1 to A6 in the appendix of this paper.
[119] The detailed comparison is displayed in Table A1 to A6 in the appendix of this paper.

which have become higher in a European context. Thus, there are substantial differences regarding (among others) coverage of expert fees and data recovery costs.

Regarding first party liability, all insurers cover crisis management expenses and data reinstatement costs. On the other hand, replacement of intellectual property, such as software, is covered by half of the insurers although this kind of reinstatement might be time-consuming and costly. Five out of seven insurers cover actual extortion payments in case of cyber extortion but related costs for investigation and prevention are only covered by two of them.

At first sight, cyber insurance coverage might look similar, but on closer scrutiny many differences in clauses exist. A direct comparison on multiple criteria such as price, coverage and deductibles is complex. Each insurance company takes its own approach towards the set-up of the contract, legal terms are explained in multiple ways by different insurers, and long lists of exceptions for coverage exist. Due to these differences in the details, it might be difficult for SMEs to acquire enough information to make an educated choice for insurance. This holds even more now most insurers solely communicate through intermediaries. Coverage is difficult to compare, not only for companies looking for insurance, but also for experts. The Authors requested experts to group insurable losses in the order of importance, and they responded that they found it too difficult to rank them.[120] This lack of uniformity complicates making a well-considered choice for a specific cyber insurance product, especially for relatively uninformed SMEs. This difficulty for potential insured to assess and compare policies, might indicate that reverse adverse selection is present. Another explanation might be that due to the complex nature of cyber risks, the insurer want to precisely define their coverage, also demanded by recent case law in the United States, as discussed in section.

Do insurers cover risks that have a likelihood of affecting their liquidity and solvency, as discussed in section III.A? Every insurer covers at least some risks that are potentially harmful for the stability of the risk pool of an insurer, when a correlated event happens. For instance, all parties incur costs for the reinstatement and replacement of data. These are costs that could be correlated when there is an exploit in a software application. Indeed, the coverage of cyber insurance inherently means that insurers to some degree must accept correlated risks. There are very few types of coverage that actually cancel out the likelihood that other parties would be affect simultaneously. This means that insurers are willing to take

[120] More information about this exploratory survey upon request.

some risk. A few parties are willing to take a higher degree of risk, in the sense that they also cover privacy liability when control of information is outsourced. This makes them potentially vulnerable for vulnerabilities in cloud platforms. Apart from that, all insurers cover risks that are typically uncorrelated, such as reputation damage. Some insurers also cover administrative fines. As section V.B discusses, insurers impose caps on payable sums, which is also considered a means to reduce the risk on insolvency flowing from catastrophic cyber incidents.

D. Caps and Deductibles

All insurers use caps. With most insurers, the insured can choose the insured amount, with the cap as maximum. The premium depends on the insured amount. For small companies, caps vary between €250,000 and €1,000,000. For large companies, there are observed caps up to €2,500,000. Indeed insurers partially expose insured to risk via caps on payable amounts.

- insert Figure 1 about here-

Figure 1 indicates that the deductibles vary between 1,000 and 100,000 euro, or between 0.40% and 4.00% of the insured amount. It can hence be rewarding for companies interested in buying insurance to take the deductible into account in their choice. The question remains however, to what extent SMEs know their risk and can participate in this kind of self selection. For example, AON applies a deductible of 0.25% of the insured amount for a company with turnover below 1 million, while Chubb's deductible for the same company is 2.50%. Most deductibles vary between 0.5% and 1% of the insured amount. It is common practice that deductibles have to be paid per insured event, not per year as might be the case in other fields of the industry. Although the precise contract conditions vary across the insurers, the difference in the height of the deductible of a factor ten suggests that insurers differ in the perception of risk attitude, that they target several parts of the market, and/or that they have different impressions of the degree of moral hazard of their customers.

The theoretical discussion in section III argued that from a social welfare perspective insurers might want to offer products with high deductibles and high caps because insured firms would like to insure low likelihood - high impact risks. However, on the contrary, the contracts observed contain relatively low caps and low deductibles. Relatively low caps for

can hinder demand for cyber insurance, because high impact risks are insufficiently insured. Moreover, relatively low caps, such as €250,000, could refrain companies from claiming, when the expected damage is significantly higher than the cap and when this damage will solely operationalize when the breach is claimed and notified. Concealing notifications and refraining from claims can for instance be present when there is high reputation damage expected in combination with low caps and when this reputation damage can be avoided by concealing the breach. Low deductibles are on first sight attractive for buyers of cyber insurance, but not really necessary, since low impact risks are bearable by the SME itself. High deductibles on the other hand allow for lower prices, more customers and hence more data which might lead to a more attractive product and lower prices.

E. Risk Reduction Measures

Only AIG and ACE have positive moral hazard clauses that lay down general requirements for firms in order to receive compensation for losses. There is no relation between such clauses and the premium, and there are no bonus/malus arrangements identified. AIG requires that the insured party takes all 'reasonable steps' to meet the standards described in the request form. Data recovery possibilities have to be tested every six months. ACE requires that the insured party makes a back-up every week, of which a copy must be saved outside the firm in a location protected against fire and water. Permanent anti-virus software has to be installed and activated and weekly updated. The deliberate use of illegal or unlicensed programs is prohibited. So, only two out of the total of seven observed insurers aim to reduce risk at the insurer. Targeted risk reduction requirements are one of the main welfare enhancing capabilities of the insurer. In that sense the limited amount of risk reduction requirements is a missed opportunity. This can be caused by the fact that that limited claim data hinders cyber insurers to make accurate risk reduction requirements for the insurance pool. This does not mean that other insurers do not have strategies at all to reduce the moral hazard problem. We did observe deductibles and caps, which are also considered to reduce moral hazard.

F. Insurers and Their Strategies

We observed nine insurers that offer cyber insurance policies for SMEs in the Netherlands. HDI-Gerling has a limited insurance product focusing on banking fraud, XL did not respond

to the request for a policy and AIG and AON offer identical products for different prices. Hence, de facto, there are six different insurers in the market when it comes to coverage. This is indeed a limited number when compared to other Dutch insurance sectors. The Dutch Association of Insurers reports 149 insurers active in the non-life sector.[121] Property insurance is offered by 78, liability insurance by 41 and motor vehicle insurance by 36 insurers. All insurers that offer cyber policies are large insurance companies that are diversified and capable of taking some losses.

The question for discussion remains whether the cyber insurance market observed by this case study contributes to social welfare because of risk transfer and reduction. The discussion argues that there is currently a mixed view as to whether the market is capable of increasing social welfare. It is beyond dispute that the insurers observed apparently perceive opportunity for some producer surplus, in the sense that they are willing to penetrate the market by offering products. The main point for discussion is whether the insurance products are capable of breaking through the aforementioned 'catch-22' situation. The theoretical framework formulated two strategies that insurers can pursue. In the first scenario, risk prone insurers aggressively penetrate the market with easy requesting procedures and an attractive price/coverage ratio. In a second scenario, a risk averse insurer primarily focusses on offering products that mitigate its own risks by insurer ambiguity, high prices and rigorous adverse selection, possibly supported by sustaining a reverse market for lemons in order to maximize its own profits.

We observed some elements of the first scenario in actual cyber insurance contracts. For instance, AON and Hiscox offered very easy cyber insurance requesting procedures, a request can be sent through a simple e-form, aiming at an efficient customer journey and all insurers cover elements of first and third party coverage. We also observed elements of the second scenario, for instance because for other insurers than AON and Hiscox, requesting cyber insurance was a time consuming process. Chubb for instance requires much insight in the company (ten pages of questions about the current state of cyber protection have to be filled out). This possibly has negatively externalities towards insurers with an easy cyber insurance requesting procedure, as possible clients might want to compare more than two products and drop out of the pool.

Prices are closely related to deductibles and caps. It is impossible to assess whether prices are attractive enough for insurers, because only an actual market equilibrium could

[121] Verbond van Verzekeraars, supra note 62.

reveal that. Anecdotic evidence from insurers itself and the co-designed survey (see section III.B) suggests that at present SMEs have limited willingness to pay for cyber insurance. Possibly this is caused, among others, by the fact that prices still are too high and do not fall in a 'nobrainer' category such as the aforementioned prices for corporate liability insurance or property insurance.[122] As argued, currently deductibles and caps are relatively low. From a social welfare perspective, one might want to increase the deductible (and cap) in order to shift the insurable risk into a more low likelihood high impact category.

De facto, a reverse market for lemons (reverse adverse selection) exists in the sense that insurance contracts are mostly difficult to request. Moreover, prices and coverage are difficult to compare. It took the Authors four months to get an overview of the market. For example, Hiscox and Chubb both offer cyber insurance in the Netherlands against comparable premiums: 0.34% and 0.35% of the insured amount. There are however considerable differences in deductibles (Hiscox 0.6% versus Chubb 2.5% of the insured amount). In addition, the exact coverage offered by the two insurers shows important differences.[123] Hiscox covers administrative fines for non-compliance with Data Protection Law, while Chubb does not, and, vice versa, solely Chubb covers vicarious liability, when IT systems are outsourced. We could not observe however whether this 'market for lemons' is the consequence of a deliberate attempt to increase information asymmetry or whether it is a result of overall uncertainty or different strategies of insurers in the market. Insurers at the moment do not use standardized or identical coverage. This would increase competition because consumers can better compare coverage and pricing details and aggregate data in order to better protect risks. On the other hand, standard forms may also prevent competition and quick response to new developments in the market.[124]

A missed opportunity is the limited amount of risk reduction / moral hazard measures. As said, we only observed two companies that set incentives for careful behavior. This might also be caused by the fact that there is little claim data and hence little inferences could be made about which risk reduction requirements are effective for the insurance pool.

Overall, what can insurance law literature and legal practitioners learn from this research? It seems that insurers approach the market for cyber risks in two ways. On the one hand, we observed a more traditional insurer approach, where a lot of information is asked to

[122] With these types of insurance, the relationship between the premium and the pay-out in case of an accident is so huge that almost everyone would find it smart to buy such insurance.
[123] The detailed comparison is displayed in Table A1 to A6 in the appendix of this paper.
[124] Avraham, supra note 49.

reduce the risk on adverse selection, possibly driven by the fact that insurer contracts are drafted by experts on more traditional insurance products. On the other hand, we observed some elements that, at least theoretically, could lead to a higher likelihood of a market to develop, such as easy access of insurance products and moral hazard measures.

VI. Conclusions, Recommendations and Further Research

This contribution formulated a theoretical framework to analyze whether current cyber insurance contracts contribute to social welfare. We also observed actual cyber insurance contracts. Some elements in those contracts foster growth from an insurance law and economics perspective, such as the sometimes simple requesting procedure and the arguably lower prices for products than several years ago. But we also identified several impediments to social welfare surplus, which can be theoretically derived from combining cyber risk literature with insurance law and economics, but are present in an unusual mix. Insurers currently insufficiently focus their coverage on low impact high likelihood risks, possibly driven by a lack of information in the market. We also observed that it is currently hard for most SME to make a well-informed choice, although this should be analyzed in future empirical research on potential buyers of insurance products. This is either a deliberate sustainment of a reverse market for lemons, or the result of the fact that the development of the market is in an early stage which results in a variety of different types of coverage in combination with recent case law (in the US) that demand a very accurate definition of coverage. Also the fact that there are only 2 out of 7 insurers observed that require risk reduction measures is an impediment for social welfare growth. Therefore, we believe that insurers currently halt between two options. The first option being a strategy of rigorous market penetration with easily accessible and attractive insurance products. The second option being significant hedging of correlated risks that reduces the potential of cyber insurance.

This research on cyber insurance contracts opens various avenues for future research and for improvement in the contribution of cyber insurance to social welfare. This section briefly discuses research on the topics of basic cyber insurance policies, mandatory disclosure of claim data, requesting procedures, cyber pooling, correlated risks and catastrophic upsides, the impact of data breach notification laws and the overlap of cyber insurance with other insurance policies.

As it is difficult to compare the existing policies, it would be interesting to study the possibility of a basic cyber insurance policy that covers the most important and/or frequent

cyber risks. With such a basic coverage, insurers only have to be compared on price and deductibles and not on complicated and widely differing coverage clauses. At the same time, the most important and frequent forms of cyber damage would then be covered, which reduces the risk of companies who have bought insurance to actually not be insured for such risks due to overlooked exclusion clauses. Additional insurance (either for other types of risks, types of losses, or higher amounts) could then be added to this basic insurance. Such an approach can be beneficial in fighting adverse selection, because firms with lower risks (such as the bakery that was included in this research) might only take the basic insurance, whereas other firms may decide to buy add-ons.

In order to tackle the problem of data unavailability, one could consider mandatory disclosure of claim data. This would make more data available faster, which could enable insurance companies to build better products because they can better estimate the distribution of risk of their portfolio. Simultaneously, it could solve issues concerning exaggeration of cyber risk as a sales strategy. However, due to the possible disadvantages of the forced nature of mandatory disclosure, more research in this direction is needed.

The requesting procedures for cyber insurance for SMEs are often very time-consuming and complicated. We recommend investigating which questions are essential in order to create a sufficient risk profile, to enable a simpler requesting procedure. Possibly, the market will correct itself in the sense that insurers that do not offer simpler requesting procedures will not gain market share.

It is worth analyzing alternatives for cyber insurance. Common solutions to the issues of systemic risks are co-operation between insurance companies on data sharing, re-insurance of risks, mandatory insurance, pooling of risks and state intervention.[125] Several scholars have argued that in particular pooling between companies is a potentially more efficient alternative because it eliminates transactions costs and overhead costs of the insurer.[126] Future research could focus on the consumer side of cyber insurance to compare the willingness to buy cyber insurance with other possibilities for risk sharing, such as pooling.

In order to contribute to the broad stream of literature that studies the systemic element of cyber risks, it would be very interesting to research empirically what the degree of correlation is between cyber risks. This is closely connected to research that focuses on the potential opportunity for governments to compensate a catastrophic cyber risk upside in order foster cyber insurance market development.

[125] Faure & Hartlief, supra note 27.
[126] See the discussion in section III.C of this contribution.

From an insurance law and economics perspective, it would be interesting to investigate to what extent the implementation of further reaching data breach notification laws is likely to drive the European cyber insurance market.[127] Furthermore, it is worth investigating the overlap of cyber insurance with traditional property insurance. Many SMEs have the perception that cyber risks are already covered by traditional insurances.[128]

Of course, given the rapidly changing nature of the Internet, the results are a snapshot and it is not unlikely that the premiums analyzed in the case study will differ in the future. In addition, the Authors requested a limited number of contracts on behalf of a limited number of organizations, so that generalizations should be made with care. Furthermore, this case study only observed one national market, in order to avoid that differences between policies are due to underlying national factors (such as legislation) that may differ between countries. However, given that cyber risk is an international phenomenon that does not stop at national borders and because the insurers investigated all are international companies, the results found for the case study in the Netherlands are likely relevant for other countries as well.

[127] Proposal 2012/0011 of the European Commission. On January 1 2016, a national data breach notification law entered into force in the Netherlands, with fines for non-compliance up to €810.000.

[128] Verbond van Verzekeraars, Dutch Insurance Industry in Figures (2014), https://www.verzekeraars.nl/verzekeringsbranche/cijfers/Documents/VerzekerdVanCijfers/2014/Verzekerd%20van%20Cijfers%202014%20%28EN%29.pdf (accessed 21 March 2016).

Tables and figures

Table 1: Correlated Risks versus Cascade Effects from the Perspective of the Insured

	Cascade effects (many third parties are hit) ⬇	
Correlated risk (identical risk operationalizes at many other insured) ⬇	No	Yes
No	Perfectly insurable	Third party coverage important / caps provide a simple mitigation of risk.
Yes	First party coverage is imposing the insurer to systemic uncertainties.	Both third party coverage as well as first party coverage

Table 2: Premiums as Percentage of the Insured Amount

Insurer	*Small (< 1M Euro)*	*Large (> 1M Euro)*
ACE	0.53%	0.53% - 0.75%
AIG	0.33%	0.40% - 0.56%
Allianz	No response (but the Authors did receive coverage)	
AON	0.26%	0.32% - 0.36%
Chubb	0.35%	0.35% - 0.99%
CNA	> 0.50% (incomplete information)	
HDI-Gerling	Only coverage for online banking fraud	
Hiscox	0.34%	0.34% - 0.74%
XL	*No response*	

Table 3: Coverage Clauses and Number of Insurers Providing Coverage

Coverage	*Cause of cyber loss*	*Insured Losses*	*Covered (out of 7 insurers)*
Third party liability			
Privacy liability	Disclosure of confidential information collected or handled by the firm or under its care, custody or control	Legal liability	7
		Vicarious liability	2
		Crisis control	7
Network security liability	Insertion of computer viruses / unauthorised access of the insured causing damage to third's systems / disturbance of authorised access by clients / misappropriation of intellectual property	Cost resulting from reinstatement	5
		Cost resulting from legal proceeding	4
Intellectual property	Breach of software, trademark and media exposures (libel, etc.)	Legal liability	3
First party liability			
Crisis management	All hostile attacks on information and technology assets	Costs to reinstate reputation	7
		Cost for notification of stakeholders and continuous monitoring	7
Business interruption	Denial-of-service attack / hacking	Cost resulting from reinstatement	5
		Loss of profit	5
Data asset protection	Change / destruction of information assets and other intangible assets	Cost resulting from reinstatement and replacement of data	7
		Cost resulting from reinstatement and replacement of intellectual property	4
Cyber extortion	Extortion to release, change, damage, destroy or transfer information / technology assets	Cost of extortion payment	5
		Cost related to avoid extortion	2

Figure 1: Premiums and Deductibles

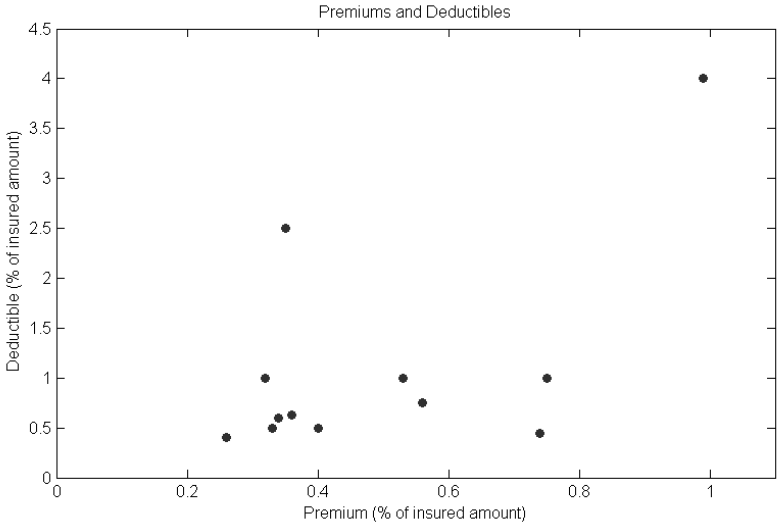

Table A1: Coverage of Third Party Liability per Insurer

Coverage	*Cause of cyber loss*	*Insured Losses*	*Comments on the interpretation*	#	*ACE*	*AIG/ AON*	*Allianz*	*CNA*	*Chubb*	*Hiscox*
Privacy liability	Disclosure of confidential information collected or handled by the firm or under its care, custody or control (e.g. due to negligence, intentional acts, loss, theft by employees)	Legal liability (also defence and claim expenses (fines), regulatory defence costs)		7	Y	Y	Y	Y	Y	Y
		Vicarious liability (when control of information is outsourced)	If not mentioned in the policy, it is assumed that the loss is not insured	2	N	N	Y	N	Y	N
		Crisis control (e.g. cost of notifying stakeholders, investigations, forensic and public relations expenses)	Consultants (legal, IT, forensic, PR) and notification/ monitoring costs	7	Y	Y	Y	Y	Y	Y
Network security liability	Unintentional insertion of computer viruses / unauthorised access of the insured causing damage to a third party, disturbance of authorised access by clients, misappropriation of intellectual property	Cost resulting from reinstatement	Recovery costs caused by insurer's behaviour or system/security errors	5	Y	N	Y	Y	Y	Y
		Cost resulting from legal proceeding	Consultant for legal advice	4	Y	N	Y	Y	Y	N
Intellectual property and media breaches	Breach of software, trademark and media exposures (libel, etc.)	Legal liability (also defence and claims expenses (fines), regulatory defence costs)		3	Y	O	Y	Y	N	N

NOTE: 'Y' is stated when coverage is provided, 'N' when no coverage is provided, and 'O' when optional coverage is offered. Insurers AIG and AON use the same policy for cyber insurance.

Table A2: Coverage of First Party Liability per Insurer

Coverage	*Cause of cyber loss*	*Insured Losses*	*Comments on the interpretation*	#	*ACE*	*AIG/ AON*	*Allianz*	*CNA*	*Chubb*	*Hiscox*
Crisis management	All hostile attacks on information and technology assets	Costs from specialised service provider to reinstate reputation	Expenses Public Relations consultant	7	Y	Y	Y	Y	Y	Y
		Cost for notification of stakeholders and continuous monitoring (e.g. credit card usage)	1. Notification and 2. Monitoring services	7	Y	Y	Y	Y	Y	Y
Business interruption	Denial-of-service attack / hacking	Cost resulting from reinstatement		5	Y	O	Y	Y	Y	Y
		Loss of profit		5	Y	O	Y	Y	Y	Y
Data asset protection	Information assets are changed, corrupted or destroyed by a computer attack / damage or destruction of other intangible assets (e.g. software applications)	Cost resulting from reinstatement and replacement of data		7	Y	Y	Y	Y	Y	Y
		Cost resulting from reinstatement and replacement of intellectual property (e.g. software)		4	Y	N	Y	Y	N	Y
Cyber extortion	Extortion to release or transfer information or technology assets such as sensitive data / to change, damage or destroy information or technology assets / to disturb or disrupt services	Cost of extortion payment	Only the payment	5	Y	O	Y	Y	Y	Y
		Cost related to avoid extortion (investigative costs)	Investigation, prevention	2	N	O	N	Y	N	Y

Table A3: Details of Coverage of Third Party Liability for ACE, AIG/AON and Allianz

Coverage	*Insured Losses*	*ACE*	*Notes*	*AIG/ AON*	*Notes*	*CNA*	*Notes*
Privacy liability	Legal liability (also defence and claim expenses (fines), regulatory defence costs)	Y	4.1, p15, an (administrative) fine is excluded ex 6.13 p.16 and ex 4 p. 28	Y	Claims: 1.4.1 Defence costs and regulatory fines, deductable is 10% of fine with a of minimum 50k, sublimit of 500k (1.3.2)	Y	Liability (2.2) and fines (2.6)
	Vicarious liability (when control of information is outsourced)	N	Not mentioned	N	Not included, not excluded	N	Not mentioned
	Crisis control (e.g. cost of notifying stakeholders, investigations, forensic and public relations expenses)	Y	p. 5 (under first party liability)	Y	First response (legal advice, IT advice, costs related to reputation management)	Y	1.6, 1.7
Network security liability	Cost resulting from reinstatement	Y	Paragraph 3, p.14	N	Not mentioned	Y	2.4b
	Cost resulting from legal proceeding	Y	Paragraph 4.1, p15	N	Not mentioned	Y	Cyber theft of money and securities explicitly included
Intellectual property and media breaches	Legal liability (also defence and claims expenses (fines), regulatory defence costs)	Y	Paragraph 4.1, p15	N	Excluded explicitly, but not for claims or defence costs following from loss of company data (2.5)	Y	Slander included (2.1)

Table A4: Details of Coverage of Third Party Liability for CNA, Chubb and Hiscox

Coverage	*Insured Losses*	*CNA*	*Notes*	*Chubb*	*Notes*	*Hiscox*	*Notes*
Privacy liability	Legal liability (also defence and claim expenses (fines), regulatory defence costs)	Y	Liability (2.2) and fines (2.6)	Y	p.5: Fines are excluded (2.3 (f) (exclusions to clauses 2-6) and the definition of clause 1: legal liability loss that does not include fines ex p.24 (ii).	Y	p.3: a civil fine is included, p.3.
	Vicarious liability (when control of information is outsourced)	N	Not mentioned	Y	p.27: A system is interpreted as also including licensed systems.	N	Not mentioned
	Crisis control (e.g. cost of notifying stakeholders, investigations, forensic and public relations expenses)	Y	Paragraph 1.6 & 1.7	Y	p.5	Y	p.3.
Network security liability	Cost resulting from reinstatement	Y	Paragraph 2.4b	Y	p.7: Legal liability loss is insured and a conduit wrongful act [which is an unauthorized access to a third party system from the system of the insured (p. 20)] is not excluded p.7 (2.1) (d) (ii) Hence third party damage is covered.	Y	p.3.
	Cost resulting from legal proceeding	Y	Cyber theft of money and securities explicitly is included.	Y	Idem.	N	Not mentioned
Intellectual property and media breaches	Legal liability (also defence and claims expenses (fines), regulatory defence costs)	Y	Slander is included (Paragraph 2.1).	N	p.8, paragraph 2.2 (f): Content Wrongful Act, infringing intellectual property (p.20), and Reputational Wrongful Act (Slander/Defamation p.26) are excluded.	N	Not mentioned

Table A5: Details of Coverage of First Party Liability for ACE, AIG/AON, and Allianz

Coverage	*Insured Losses*	*ACE*	*Notes*	*AIG/ AON*	*Notes*	*CNA*	*Notes*
Crisis management	Costs from specialised service provider to reinstate reputation	Y	paragraph 4,p15	Y	First response (legal advice, IT advice, costs related to reputation management)	Y	paragraph 1.9
	Cost for notification of stakeholders and continuous monitoring (e.g. credit card usage)	Y	paragraph 4, p5	Y	Including call enter up to 6 months after reporting (1.2.6) and premiums for identity fraud insurances up to 2 years after reporting (1.2.7)	Y	3.50 (f) (ii) credit monitoring services for a period of up to six months following the date of such Privacy Breach or Data Breach
Business interruption	Cost resulting from reinstatement	Y	Not mentioned	N	Optional	Y	paragraph 1.6
	Loss of profit	Y	"cost to avoid loss of profit are insured" , p.6. Business losses insured p.10, hence Y	N	Optional	Y	paragraph 1.6
Data asset protection	Cost resulting from reinstatement and replacement of data	Y	paragraph 4.1 p5	Y	When caused by insured or system failure: reasonable and necessary costs (1.2.4)	Y	paragraph 1.7
	Cost resulting from reinstatement and replacement of intellectual property (e.g. software)	Y	paragraph 4.1,p5	N	Only reinstatement of third person data	Y	paragraph 1.6
Cyber extortion	Cost of extortion payment	Y		N	Optional	Y	paragraph 1.8
	Cost related to avoid extortion (investigative costs)	N	Only costs directly resulting from cyber extortion	N	Optional	N	Not mentioned

Table A6: Details of Coverage of First Party Liability for Chubb, CNA, and Hiscox

Coverage	*Insured Losses*	*Chubb*	*Notes*	*CNA*	*Notes*	*Hiscox*	*Notes*
Crisis management	Costs from specialised service provider to reinstate reputation	Y	up to 12 months after reporting, 1.6	Y	Crisis management expenses means (among others) the costs of an a public relations consultant (p.20)	Y	p.4
	Cost for notification of stakeholders and continuous monitoring (e.g. credit card usage)	Y	Both in case notification is prescribed by law and in case such rules are absent (1.7)	Y	p.20 Among others: "Call centre activity and information security forensic investigator"	Y	p.4
Business interruption	Cost resulting from reinstatement	Y	paragraph 1.2	Y	p.5	Y	p.4
	Loss of profit	Y	paragraph 1.2	Y	p.5	Y	p.4
Data asset protection	Cost resulting from reinstatement and replacement of data	Y	paragraph 1.1	Y	"reasonable" Recovery expenses for E-Business interruption are covered (p.5 clause 3 and p.26)	Y	p.5
	Cost resulting from reinstatement and replacement of intellectual property (e.g. software)	Y	paragraph 1.1	N	"reasonable" Recovery expenses for E-Business interruption are covered (p.5 clause 3 and p.26); system replacement not covered (2.3d)	Y	p.5
Cyber extortion	Cost of extortion payment	Y	paragraph 1.4	Y	p.22	Y	p.5
	Cost related to avoid extortion (investigative costs)	Y	paragraph 1.4	N	p.22	Y	p.5