The Law and Economics of Cyber Security

De rechtseconomie van internetveiligheid

Proefschrift ter verkrijging van de graad van doctor aan de
Erasmus Universiteit Rotterdam op gezag van
de rector magnificus
Prof.dr. R.C.M.E. Engels
en volgens besluit van het College voor Promoties

De openbare verdediging zal plaatsvinden op
maandag 25 juni 2018 om 10.00 uur
door

Bernoldus Franciscus Hendrikus Nieuwesteeg
geboren te Utrecht, Nederland

Erasmus University Rotterdam

Promotiecommissie

Promotor:	Prof.mr.dr. L.T. Visscher
Overige leden:	Prof.dr. E.F. Stamhuis
	Prof.dr. M.J.G. van Eeten
	Prof.dr. E. Santarelli
Co-promotor:	Mr.dr. C. van Noortwijk

This thesis was written as part of the European Doctorate in Law and Economics programme

An international collaboration between the Universities of Bologna, Hamburg and Rotterdam.
As part of this programme, the thesis has been submitted to the Universities of Bologna, Hamburg and Rotterdam to obtain a doctoral degree.

This study is printed in Palatino Linotype.
This font is designed by Hermann Zapf. He named it after Giambattista Palatino, a calligrapher living in the time of Leonardo da Vinci. The letters appear to be larger, because of the open and spacious design.

The Law and Economics of Cyber Security

Bernold Nieuwesteeg

Acknowledgements

It is late 2011. I knock on the door of prof. Michel van Eeten because I am curious about his research in cyber security. The conversation is good. As a consequence, in 2012, I write a master thesis studying the economics of data breach notification laws. In 2013, Michel emails me with the following message: "I do not know whether you want to pursue a PhD, but this might be something for you." In hindsight, this could not be more of an understatement. When following up on the email, prof. Michael Faure and prof. Louis Visscher introduce me the world of the European Doctorate of Law and Economics. Again, the conversation is good. Consequently, I start this adventurous research project that aims to connect the world of law and economics with the cyber security theatre in 2014. Now, it is the year 2018 and this work has been finished. Michel, Michael and Louis, during these seven fat years you provided me with indispensable guidance, inspiration and momentum. Thank you.

I also sincerely would like to thank my co-promotor Kees van Noortwijk, with whom I had the pleasure to give several lectures in the economics of cyber security and privacy, for his valuable and essential feedback. My gratitude also goes to the members of the EDLE faculty, for instance Joe Rieff, Giulia Barbanente, Orlin Yalnazov, Ignacio Cofone, prof. Sharon Oded, Marco Fabbri and prof. Klaus Heine for their readiness in providing support or inspiration when deemed appropriate. Marianne Breijer, Simone Rettig, Reini van de Sandt and Aimée Steenstra Toussaint provided the logistical foundation that made this entire research endeavour possible. I would like to thank profoundly Bob de Waard, with whom I had the pleasure to cooperate in many ways. I thank Leonard van der Leeden, Nathalie Ahsmann and especially Teun Steenbergen for their great editorial support during the empirical and final parts of the study.

The study benefited enormously from the intense cooperation and information diffusion with government, industry and other universities. My gratitude goes to the experts from SURF, the Dutch National Cyber Security Centre, the Leiden - Delft - Erasmus Centre for Safety and Security and the Economics of Cyber Security group at Delft University, with whom I intensively cooperated. I am very grateful to the more than 50 experts that reserved time to be interviewed in the context of this study. Also, I should not forget to thank the many (sometimes anonymous) reviewers for their feedback, when presenting parts of this study at workshops, conferences and symposia.

Sometimes people gave seemingly small suggestions that later on proved of vital importance for the overall process or end-product of this study. The suggestions of Christof Abspoel, Bram Eidhof, Eric de Kruijk, Tijmen Klein Bronsvoort, Dennis Ramondt, Willem Both, Catherine Endtz, Jaap Cohen, Renée Visser and prof. Nico van Eijk truly acted as butterflies that caused a great effect. Also, I could not have written this study without the energy and short-term rewards that inherently result from the practice of building businesses with Josje Damsma. I would like to praise my friends from high school (musketiers), law school (broederschapp), model united nations (goffies), theatre (bureau klein leed), de Nationale DenkTank (tijgers), the Samara summer school in rocket engineering (HTM) and other places for tolerating me the past four (or probably even more) years. Finally, I would like to thank my family, especially my mother, father, brother, second cousin and great aunt for their enduring support.

Table of Contents

Detailed Table of Contents

List of Acronyms and Abbreviations

CEO	Chief Executive Officer
CIA	Confidentiality Integrity Availability
CISO	Chief Information Security Officer
Charter	Charter of Fundamental Rights of the European Union
CSR	Corporate Social Responsibility
DBNL	Data Breach Notification Law
DPL	Data Protection Law
DPRK	Democratic People's Republic of Korea
DPA	Data Protection Authority
DPO	Data Protection Officer
EALE	European Association of Law and Economics
EC	European Commission
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation (Regulation 2016/67)
ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
MS	Member State of the European Union
MSS	Managed Security Service
NCSC	National Cyber Security Centre
NIS	Network and Information Security
NSA	National Security Agency
OPOL	Offshore Pollution Liability Agreement
P&I Club	Protection and Indemnity Club
QTA	Quantitative Text Analysis
SaaS	Software as a Service
SME	Small and Medium Enterprise
TEU	Treaty on European Union
WEIS	Workshop on the Economics of Information Security

List of Tables

List of Figures

SETTING THE STAGE:

THE CYBER SECURITY THEATRE

1. INTRODUCTION

1.1. Introduction

It is June 2017 and I am writing this introduction. The Wannacry and NotPetya cyber attacks dominate world news and their impact is colossal. Wannacry infects over 300,000 computers.[1] NotPetya disrupts a quarter of the Rotterdam harbour for six days and its total cost estimations exceed €100 million.[2] The world sees, more than ever before, that cybercriminals can relentlessly punish suboptimal security. Wannacry and NotPetya also show that there is a problem with information in cyber security. How can it be that some organizations suffered huge amounts of damage while others suffered hardly any harm at all? Apparently, Telefónica, FedEx, Deutsche Bahn, Maersk, DLA-Piper and Vodafone and many other organisations that were hit in these sunny days in June did not install the right patch that could have done the job (and which was already available for a few months).[3] But was it really as simple as that? Large organization have

---

[1] Lawrence and Robertson (2017) <https://www.bloomberg.com/news/articles/2017-05-18/the-wannacry-global-hack-could-have-been-much-much-worse> (accessed 30 March 2018).

[2] Verschuren (2017) <https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693> (accessed 30 March 2018, Dutch); Bekker (2017). <http://www.apmtrupdate.com/update-gate-open-247-this-weekend-for-truck-import-pick-up-and-export-delivery-at-apm-terminals-rotterdam/> (accessed 30 March 2018, Dutch); Sedee (2017) <https://www.nrc.nl/nieuws/2017/06/27/volg-hier-de-ontwikkelingen-rond-de-wereldwijde-randsomware-aanval-a1564740)> (accessed 30 March 2018, Dutch). I will use the Wannacry and NotPetya throughout the study as an example to clarify the nature of cyber risk.

[3] Schuetz, Robertson and Grant (2017) <https://www.bloomberg.com/news/articles/2017-06-28/cyberattack-starts-causing-real-consequences-with-fedex-ports> (accessed 30 March 2018); Goodin (2017) <https://arstechnica.co.uk/information-technology/2017/05/what-is-wanna-decryptor-wcry-ransomware-nsa-eternalblue/> (accessed 30 March 2018); De

to install tens of thousands of patches per year. Installing them all immediately would significantly hamper business availability and continuity, possibly more than the attacks they are preventing. An appropriate cyber security strategy is not straightforward and hence, organisations have to learn from each other.

Accordingly, the mere examples Wannacry and NotPetya demonstrate the importance of the studies' main ambition to analyse the stimulation of information diffusion in cyber security in order to improve the cyber security investment strategy of organizations. In the aftermath of these attacks, a German journalist discovered an interesting detail. The name 'Petya' was possibly inspired by the 1995 James Bond film 'Goldeneye'. In the film, NotPetya is a satellite that carries an atomic bomb called 'Goldeneye'. It is thought provoking that the chosen metaphor actually quite accurately resembles the devastating impact of cyber attacks, since the systemic element of cyber risk has in fact many similarities with risk of a nuclear attack from space. To put it simply, it can potentially happen anywhere and affect anyone using devices connected to the Internet. The detail was discovered, because one of the cybercriminals responsible for developing NotPetya allegedly had a twitter account with an image of the Russian hacker Boris Grishenko, the antagonist in the James Bond film.[4] At least he or she made theatrical appearance in the cyber security theatre, in which I also welcome the reader.[5]

Brauw Blackstone Westbroek (2017) <https://www.debrauw.com/newsletter/wannacry-petya-attacks-consequences-trends-tackling-ransomware-threats/#> (accessed 30 March 2018).

[4] Scherschel (2016) <https://www.heise.de/newsticker/meldung/Petya-Mischa-Goldeneye-Die-Erpresser-sind-Nerds-3571937.html> (accessed 30 March 2018).

[5] The term 'Security theatre stems from the practice of investing in security in order to provide the perception or feeling of security improvements (Schneier

We will now enter its stage: in the upcoming eight chapters I will analyse two types of legal instruments, being regulation[6] and contract.[7] Both instruments have the potential of correcting market failures in the cyber security market. Primarily, these instruments can reduce the current information deficit because they potentially enhance incentives for organizations to engage in cyber security *information diffusion*.[8] Information diffusion is the continuous circulation of information related to the return on cyber security investments and the nature of cyber security risk in order to attain optimal cyber security. It leads to many benefits for organizations and society as a whole. To name a few: Increased information diffusion leads to increased efficiency in cyber security investments, because organizations can utilise information from other organizations and do not have to 'reinvent the wheel'.[9] Also, increased diffusion of data leads to better products, such as cyber insurance. Further, it balances market power of big software and

---

(2003)). In war, a theatre can mean a designated arena where significant military events happen, such as 'airspace' or the eastern front in World War II (Von Clausewitz (1832)). Ironically, the defence of Berlin by the Nazis in April 1945 had the code word 'Fall Clausewitz' and the capture of Berlin by the Soviets ended the Eastern front. Within the study, I shall occasionally refer to the term 'cyber security theatre' as the distinguished arena of cyber security with its particular technical (Section 1.3.2, 1.3.3, 1.3.4), economical (Section 1.5) and legal (Chapter 2, Section 2.3) dynamics.

[6] Data Protection Regulation (Part I) and within this regulation, data breach notification laws (Part II)

[7] The risk shifting agreement, either from a risk transfer perspective (cyber insurance) or risk sharing perspective (cyber risk pooling), both discussed in part III.

[8] Sometimes the study also uses the term knowledge diffusion interchangeably with the term information diffusion.

[9] As long as the costs of information diffusion are not higher than the benefits of not reinventing the wheel. Information diffusion realigns incentives and corrects market failures as I shall argue in Chapter 2.

security firms which end up with fewer possibilities for exploiting their information advantage at the expense of the competition. And, when information diffusion reduces transaction costs, this could lead to a reduction of the externality problem.[10] Unfortunately, the status quo yields suboptimal spontaneous diffusion of information. Information diffusion has strong public good characteristics, which means that the actor that diffuses the information will not or limitedly benefit from it. Information diffusion can even harm organizations, for instance when the information diffused contains data breaches that can negatively affect the reputation of the organization.

Thus, the study starts from the argument that stimulating information diffusion is indispensable for attaining optimal cyber security. However, the complexity of cyber security prevents straightforward solutions that effortlessly incentivise organizations to share their best practices. I will argue that the cyber security theatre is characterised by a high speed of change in cyber risk, misaligned incentives, inherent insecurity, information deficits, a high risk of regulatory failure and market power of big software and security firms. This leads to one of the study's main claims that the three main societal actors - university, government and industry - must work together.[11] Consequently, I will study the role and responsibility in stimulating information diffusion for all three parts of this triple helix. I will study how these three parties can stimulate information diffusion in order to increase social

---

[10] Coase (1960).

[11] These are the parties that should join together for optimal societal innovation. This so-called *triple helix approach* is brought into play because not a single part of society can solve the puzzle because information diffusion in cyber security is too complex. The three helices can and should complement each other. Chapter 2, Section 2.4 will further elaborate on the triple helix approach.

welfare.[12] The goal is to attain optimal security, not perfect security, which centralises in the concept of 'efficiency'.[13] The social welfare analysis aimed at reaching efficiency that is practiced in the study is the starting point of much research in law and economics.[14] However, I will apply the social welfare analysis to a new theatre that has not been explored sufficiently in the law and economics literature.[15] The focus on information diffusion in combination with the triple helix approach results in the following research question:

> *How can university, government and industry efficiently stimulate cyber security information diffusion?*

Closely connected to the main research question, the study has three overarching ambitions.

> **Ambition 1:** Contributing to the literature on data protection laws (Part I), data breach notification laws (Part II) and risk shifting agreements (Part III).

The study is divided in three parts that cover several *cases* that contribute to the literature. The three parts are mutually exclusive in

---

[12] See Chapter 2, Section 2.4
[13] Cooter and Ulen (2016).
[14] Posner (1972), pp. 29-96; Shavell (1980), pp. 1-25; Shavell (2004); Landes and Posner (1987); Cooter and Ulen (2004); Schäfer and Ott (2005); Shavell (1987); Brown (1973), pp. 323-350; Polinsky (1980), pp. 363-370; Faure (2009).
[15] This does not withstand the fact that there has been literature that aims to study cyber security from a law and economics perspective. Compare for instance a study with the same title as this study by Grady and Parisi (2005). However, this study did not include a discussion of the specific microeconomic phenomena in cyber security identified by the economics of cyber security that will be discussed Section 1.5. This study will naturally include the relevant law and economics literature where most appropriate.

the fact that they all focus on means for stimulating information diffusion corresponding to the separate societal roles and tools that each of three parties have. Part I starts with the role of university. One could argue that 'academia' or 'science' would be a better term for this part. However, the triple helix literature consistently uses the term 'university' and therefore I will use this term. Within the university helix, I focus on one legal instrument, being the data protection regulation. As an example of the contribution university could make to the assessment of this legal instrument, I will perform a quantitative text analysis (hereafter: QTA) to better compare laws concerning this subject and unlock them for further statistical analysis in academia. This part thus focuses on information diffusion *about* a legal instrument. This part acts as an example of one of the available academic tools that can stimulate information diffusion. The performance of the tool as such is not scrutinised. Part II continues with the role of governments. This part focuses on one obligation within data protection regulation, the data breach notification law (hereafter: DBNL). This is an obligation to notify data breaches in due time to the data protection authority (hereafter: DPA) and consumers. I will analyse to what extent the upcoming EU DBNL contributes to information diffusion and social welfare. Part III will analyse the role of industry.[16] Also here, I will limit myself to two cases where the contractual freedom of parties could lead to fruitful results in the sphere of information diffusion. I will analyse the role of two risk shifting contracts. These are risk transfer contracts (cyber insurance, Chapter 6) and risk sharing contracts (cyber risk pooling[17], Chapter 7). Hence, both Part II and Part III scrutinize examples of tools, utilizable by government and industry, which can stimulate information

[16] By industry I mean organizations in general, not cyber security industry in specific.

[17] Risk sharing without the interference of an insurer.

diffusion, while Part I performs an example of a tool university can employ without scrutinizing the execution of the performance as such.[18] Figure 1 displays the structure of the study.

Figure 1: Structure of the study

> **Ambition 2:** Proposing an agenda concerning the stimulation of information diffusion in cyber security for the university, government and industry triple helix.

After the deep-dives in the three substantive parts, the study synthesizes the different roles, responsibilities and tools of the triple helix to stimulate information diffusion in cyber security. I will show that the deployment of the individual tools of these three parties will yield a fruitful contribution to social welfare and optimal security. Consequently, an agenda concerning the stimulation of information diffusion in cyber security for university, government and industry emerges. This agenda serves as a guideline for future research in the law and economics of cyber security.

---

[18] Chapter 2, Section 2.4 will further elaborate on the connections between the parts of the study

Ambition 3: Connecting law and economics with the economics of cyber security.

It is my third ambition to engrain the linkage between the field of *law and economics* and the field of *economics of cyber security*. *Law and Economics* has been founded in 1961 by two independently written seminal papers of Ronald Coase and Guido Calabresi.[19] It primarily focuses on the application of microeconomic theory to scrutinize the efficiency of legislation. Law and economics theory has strong foundations in the United States, where it is the primary field of legal scholarship. The genesis of the *economics of cyber security*[20] can be attributed to Ross Anderson, who wrote a seminal paper in 2001.[21] The core thought of the economics of cyber security is that microeconomic theory can better explain the challenges in cyber security than a technical approach. The economics of cyber security has a strong empirical and pragmatic component.[22] Scholars in the economics of cyber security should benefit from the development of theory and methodology within law and economics. Scholars in law and economics should learn from the insights into the dynamics, empirics and microeconomic peculiarities of cyber risk as encountered in the economics of cyber security. But there is a large gap to be bridged. It is exemplary that, when either field does research on the intersection of

---

[19] Coase (1960); Calabresi (1961).

[20] The economics of cyber security is also called the Economics of Information Security or EconInfoSec. See www.econinfosec.org

[21] Anderson (2001).

[22] As can be observed in the composition of the papers in its main leading forum, the Workshop of Economics of Information Security (WEIS). For instance, within the 2017 edition of WEIS 2017, I observed a significant empirical component in 18 out of the 23 papers that were presented. For scholars in law and economics, the economics of cyber security should not be mistaken by classical microeconomic theory development.

the two fields, currently only 4% of the references is from that other field.[23] Hence, I will propose several recommendations for the further linkage between these two fields. This *law and economics of cyber security* is the foundation that supports the other two ambitions. That is, it can further formulate a common 'cyber security information diffusion' agenda for university, government and industry. This agenda could build upon the analyses in the three substantive parts of the study.

This chapter further introduces the studies' theoretical framework and core concepts. Section 1.2 will introduce the procedural strategy and methodological approach. This includes the ambition of the study to connect law and economics with the economics of cyber security. Section 1.3 will introduce the nature of (investing in) cyber security. This section will define investing in cyber security as a means to reduce cyber risk. In addition, the section will provide a brief introduction of the characteristics and dynamics of cyber threats, vulnerabilities and the strategies to reduce them. Section 1.4 will discuss the relevance of optimal security contrary to perfect security. It will be argued that cyber security investments need to contribute to social welfare. Legal scholarship in cyber security currently infrequently applies the efficiency criterion, especially in the European Union (hereafter: EU). I will relate social welfare to fundamental rights and the techfix (the belief that cyber risk can be reduced to zero by implementing technical solutions). Section 1.5 discusses some of the main economic bottlenecks for attaining social welfare: externalities, public good characteristics, market power, and information deficits. Subsequently, Chapter 2 will focus on the specific issues related to information diffusion in cyber security; the framework that will pave the road for Parts I, II and III.

---

[23] See Section 1.2.1.

1.2. The Methodology and Procedural Strategy of the Study

The study applies law and economics to cyber security. Hence, the field of *law and economics* will intersect with the domain of *economics of cyber security*. Section 1.2.1 presents a short introduction into the origins of the two disciplines. Section 1.2.2 will introduce the comprehensive law and economics methodological toolkit used in the study. Section 1.2.3 will explicate how the study has been established.

1.2.1 Law and economics and economics of cyber security

Both law and economics and the economics of cyber security use microeconomics to study the dynamics of either the law or cyber security. There are opportunities for mutual learning between those two fields. Scholars of the economics of cyber security can learn from the application of law and economics analysis of cyber security, such as optimal enforcement and the literature regarding risk shifting agreements. Scholars in law and economics can also benefit from the insights from the economics of cyber security. This includes the core dynamics of investing in cyber security, such as threats, vulnerability, impact and strategies to reduce them. In addition, the economics of cyber security provides insights into the specific microeconomic peculiarities of the systemic cyber security risk, such as far reaching externalities, various types of stubborn information deficits and persistent market power of security firms and software companies. Without a doubt, the intersection of law and economics and economics of cyber security is fertile ground for contributions to optimal cyber security. When legal instruments are entering the cyber security theatre, scholars of law and economics and the economics of cyber security should work together in order to make sure they contribute to social welfare or at least show what the social welfare implications of these choices are. And within the context of the storyline of the study, the law and economics of cyber security should design and analyse legal instruments that contribute to information diffusion.

However, quite surprisingly, there has been little research on cyber security in law and economics[24] and there has been relatively little research on the role of the law and legal instruments in the economics of cyber security.[25] The following exploratory analysis might illuminate the lack of the current nexus between the two fields. I analysed to what extent papers in law and economics and papers in the economics of cyber security referenced to the other field. First, I reviewed the papers presented at the European Association of Law and Economics (hereafter: EALE), the main European forum for law and economics. I checked which papers analysed cyber security and subsequently, how many times these papers referred to a paper in the economics of cyber security.[26] The results are shown in Table 1.

[24] As already mentioned, the distinguished Law and Economics scholars Grady and Parisi (2005) bundled essays on cyber security, but these essays did not include the microeconomic focus of the Economics of Cyber Security. Elkin-Koren and Salzberger do the same, but their work does not include cyber security (Elkin-Koren and Salzberger (2004)).

[25] This does not withstand the fact that there is literature within the economics of cyber security research that included the law. For instance, the effects of the adoption of data breach notification laws have been measured by relating them to identity theft rates (Romanosky, Telang and Acquisti (2011), pp. 256-286). These laws have been subject to further evaluation, for instance by Bisogni (2013). Furthermore, the membership of cybercrime convention of different countries has been correlated with the amount of spam at ISP's in these countries (Van Eeten, Bauer, Asghari et al. (2010)). Also, the economics and regulation of certification authorities have been researched (Arnbak, Aghari, Van Eeten et al. (2014)). A last example is research on the cross-country independence of cyber-attacks (Wang and Kim, 2009).

[26] Proxy: presented at WEIS (Workshop on the Economics of Information Security).

Table 1: WEIS references in EALE papers

WEIS references in EALE papers						
Edition	**Number of papers about cyber security**	**Total number of papers per edition**	**Percentage**	**Number of references to WEIS**	**Cumulative number of references in these papers**	**Percentage**
2017	1	111	0.90%	4	34	11.76%
2016	2	160	1.25%	2	110	1.82%
2015	1	177	0.56%	1	32	0.56%
2014	1	132	0.76%	1	87	1.15%
2013	2	144	1.39%	2	168	1.19%
2012	0	138	0.00%			
Total:	**7**	**862**	**0.81%**	**10**	**576**	**1.74%**

As Table 1 above shows, the number of papers concerning cyber security in EALE is very limited, especially when taking into account that I was (co-)author of two of the in total seven papers.[27] This supports the argument that cyber security is not an important subfield within law and economics. Also the number of references originating from the Workshop of the Economics of Information Security (WEIS) is low, although this is likely to be a slight underestimation of the total number of references to sources related to the economics of cyber security.

[27] Nieuwesteeg and Faure (2017); Nieuwesteeg (2014).

Table 2: L&E references in WEIS papers

L&E references in WEIS papers						
Edition	**Number of papers with a legal aspect**	**Total number of papers per edition**	**Percen-tage**	**Number of references to L&E**	**Cumulative number of references in these papers**	**Percen-tage**
2017	4	23	17.39%	0	165	0.00%
2016	2	21	9.52%	0	64	0.00%
2015	4	22	18.18%	5	105	4.76%
2014	0	20	0.00%			
2013	1	20	5.00%	4	77	5.19%
2012	1	20	5.00%	6	50	12.00%
Total:	**12**	**126**	**9.52%**	**15**	**461**	**3.25%**

Secondly, I reviewed the papers presented at WEIS, the main forum for the economics of cyber security. Table 2 shows that especially the last three years, the number of papers with a legal aspect presented at WEIS is quite high given the multidisciplinary nature of the forum. Quite surprisingly, most of these more recent papers did not refer to sources in law and economics at all. As said, using WEIS references as a proxy for measuring referencing to law and economics in EALE papers, is likely to be an underestimation. Hence, the mutual referencing to both disciplines is around 3-4% of total references, when subjects are discussed that largely overlap with this other discipline (either legal or cyber security). In my view, a further connection between law and economics with the economics of cyber security is both necessary and indispensable for asking and answering research questions in the theatre where law, economics and cyber security are jointly on stage.[28] The synthesis of the study in Chapter 8 aims to

[28] Also Van Eeten and Mueller (scholars in the Economics of Cyber Security) have argued that regulatory intervention in cyber security requires understanding of

provide an interpretation on why this research area has not been sufficiently developed yet, given the low amount of literature on the intersection of law and economics and economics of cyber security.[29]

1.2.2 The core methodology and paradigm

The study uses a deductive approach based on microeconomic incentives, especially in Part II and III. Incentive analysis is the basis of economics of cyber security. Ross Anderson argued in his seminal paper 'Why Information Security is Hard': "Information Security is at least as much due to perverse incentives. Many of the problems can be explained more clearly and convincingly using the language of microeconomics".[30] Also in law and economics, incentive analysis is widely used and regarded as a key concept in research, also in cyber space. Renda states "The importance of individual incentives, social norms and the context of human behaviour in determining the effectiveness of legal rules is nowhere as tangible as in the intangible world, i.e. as in cyberspace."[31] The study uses several subsets of incentive analysis, such as the economics of deterrence and enforcement.

Part II focuses on the literature related to incentives to comply with effective legislation, such as on law and social norms[32], the economics

---

the complex interplay between law, economics and the behaviour of digital communication systems (Van Eeten and Mueller (2013), pp. 720-736).

[29] Chapter 8, Section 8.3.2 argues that this for instance can be caused by the different academic traditions in the two fields.

[30] Anderson (2001); Anderson and Moore (2007), p. 11.

[31] Renda (2011), p. 195.

[32] Posner (2000).

of deterrence[33] and the economics of enforcement.[34] Part III focuses on the literature related to incentives of risk shifting agreements, such as the law and economics of systemic risk and insurance, and the economics of cyber insurance. The incentive analysis will be supported by cost-benefit analysis.[35] This determination of cost and benefits will often not be definite, because exact costs and benefits of cyber security legal instruments are often very hard to determine[36] and differ a lot between organizations. Nonetheless, I will provide an overview of which organizational and social cost should be taken into account when scrutinizing the effectiveness of legal instruments on individual incentives.[37] Part I uses, next to the economics of deterrence, QTA to code data protection regulation.[38] QTA is an established research method designed to unlock legal texts for quantitative comparison and statistical analysis and facilitates the diffusion of information about this legal instrument.[39]

The study works with a rational actor and utilitarian paradigm. This means that actors are assumed to make consistent and predictable choices from alternatives based on their preferences and try to

---

[33] The starting point for this type of analysis is the seminal article of Gary Becker (1968) ; See also for instance: Cooter and Ulen (2016).
[34] Stigler (1974); Becker (1968).
[35] Parisi (2004), p. 259; Renda (2011).
[36] Anderson, Barton, Boehme et al. (2013), pp. 265-300.
[37] Often, already the clarification of private and social cost and benefits and the regulatory cost aware policy makers of the ramifications of their choices on social welfare.
[38] Meuwese and Versteeg (2012), pp. 231-257.
[39] For instance, quantitative text analysis has been one of the main subjects of the 2015 Hamburg Summerschool in Law and Economics. See <https://www.jura.uni-hamburg.de/media/einrichtungen/inst-recht-oekonomik/summer-school/summer-school-2015.pdf> (accessed 30 March 2018).

maximize their own utility.[40] It will not come as a surprise for the reader that the rational actor paradigm, as well as the utilitarian perspective has been challenged by among others economists, philosophers and psychologists.[41] In general I will not include these discussions in the study. Mostly, the study will focus on the role of organizations, in which behavioural biases are slightly less on the foreground and behaviour is considered to be more rational. That does not mean that behavioural biases are not playing a significant role the law and economics of cyber security. Consider the example of intolerance for ambiguity[42] in the case of DBNLs. Intolerance for ambiguity can result in an incentive to conceal data breaches because of the ambiguous perceived reputational damage that results from disclosing the data breach. However, it can also result in an incentive to disclose data breaches, to avoid the ambiguous likelihood that there will be a fine of the data breach notification authority. This is exemplary for the fact that hypotheses about the effects of behavioural biases can often work out two ways, and the exact determination of their actual direction must be subject to academic scrutiny. As said, I do not include this in the scope of the study, but I will refer to those scholars who perform these analyses where appropriate.

1.2.3 Process strategy

It is the second ambition of the study to provide an agenda for the stimulation of information diffusion in cyber security for universities, governments and industry. The study will practice what it preaches by adopting a strategy of cooperation. I have collaborated with all three helices in addition to the above-described academic methodology. The

---

[40] Bentham (1789).

[41] See for instance Holt and Laury (2002), pp. 1644-1655; Kahneman and Tversky (1979); Kahneman and Tversky (1996), pp. 582–591; Korobkin, Ulen and Title (2000).

[42] Frisch and Baron (1988), pp. 149-157.

study is the result of collaboration between the Universities of Rotterdam, Bologna, Hamburg, Delft, Leiden and Tilburg. In addition, I have worked in close collaboration with government institutions focussing on cyber security, such as the Dutch SPA, the National Cyber Security Centre (NCSC), the Dutch Cyber Security Council. I collaborated with the private organizations Arbinn, Unibarge and Eigensteil and the The Hague Security Delta for assessing the cyber insurance market, especially in Part III, which focuses on the role of industry. I have intensively cooperated with the SURF cooperation for assessing the potential of the cyber risk pooling market. The process of cooperation has fulfilled an important role in the verification, validation and iteration of results of the study. Contrary to more established fields of law and economics, a significant part of the research has not been published in peer-reviewed journals. Therefore, I conducted over 50 exploratory and semi-structured interviews that have influenced the content of all chapters in the study.[43] Next, I have designed and led a co-creation session with members of industry in order to jointly investigate preferences and prerequisites related to cyber risk pooling. Moreover, I have used surveys to support and validate the analysis in Part III. Also, most parts of the study have been presented at various academic conferences related to the Law and Economics of Cyber Security in which I also have participated as a (panel) discussant. As a next step, parts of the study have been published as separate Articles in (peer-reviewed) journals.[44] Finally, I have tried to contribute to the information diffusion about the study, for instance through book reviews, presentations and pitches at (non-) academic conferences and appearances in the media.

---

[43] A full list of the interviewees can be found in the bibliography.
[44] This will be indicated at the relevant parts.

1.3. Investing in Cyber Security

I will now start the substantive part of this introduction with an establishment of the nature of cyber risk and investing in cyber security.[45] This is the very information that needs to be diffused.[46] This section starts from the nature of cyber risk in Section 1.3.1. Sections 1.3.2 to 1.3.4 will introduce the three elements of cyber risk: threat, vulnerability and impact. Cyber risk is not isolated at an individual or organizational level, as Section 1.3.5 will illustrate.[47] Section 1.3.6 will proceed with a brief introduction of elements of modern organizational cyber security, which mostly focuses on reducing impact. Section 1.3.7 will discuss the difficulties of investing in cyber security for organizations related to the market power of software and security vendors.[48]

1.3.1 Cyber risk

What is cyber risk? Unfortunately, there is not a common agreement on its definition.[49] The study will use one of the most used definitions

---

[45] Section 1.3 has not the aim to be exhaustive, but will introduce the core concepts and dynamics of cyber security risk that are necessary for studying the upcoming parts.

[46] I am not going to be extensive in this analysis and will refer to more extensive articles, reports and other documents where deemed appropriate.

[47] The study is mostly about investing in cyber security on an organizational and societal level, although the lessons learned can also be of value for consumers. See for an extensive discussion Anderson (2008, p. 815; Within Part III, cyber risk plays an important role because the analysis focuses on how to shift it, see also Biener (2015).

[48] The concept cyber risk and its breakdowns is used extensively throughout the study, most prominently in part II and III.

[49] The definition of cyber risk is to some extent ambiguous or has at least many interpretations. See for an extensive discussion: International Organization for Standardization and International Electrotechnical Commission 2011; Haimes (2006), pp. 293-296; Byres and Lowe (2014); Caballero (2009), p. 232. See for a more historical reflections: De Leeuw and Bergstra (2007).

of cyber risk. This definition decomposes cyber risk into the elements threat, vulnerability and impact.[50]

1. The threat is the actor that can exploit a vulnerability and obtain or damage an asset.
2. The vulnerability is a weakness in a security system that can be exploited by a threat.
3. The impact is the damage to the assets of this system after the attack.

Usually, risk is defined as the product of threat, vulnerability and impact. Naturally, total cyber risk is the sum of all threats and their expected impact. Since cyber risk is the expected value of damage, the proper mathematical formula sees threat and vulnerability as a likelihood and impact as a monetary value. The mathematical definition is as follows:[51]

> Cyber security risk = Probability(Threat{likelihood to take place})* Probability(vulnerability{likelihood of being exploited})* Cost(impact)

1.3.2 Threat

The threat is the actor that can exploit a vulnerability and obtain or damage an asset. There are two main types of threats: intentional and unintentional actions. Preventing the former is called cyber security

---

[50] Also, within this definition, there is debate whether it is mutually exclusive and collectively exhaustive. See for instance Cox (2008).
[51] International Organization for Standardization and International Electrotechnical Commission 2011; Haimes (2006), pp. 293-296; Byres and Lowe (2014); Caballero (2009), p. 232.

and the latter is called cyber safety.[52] Cyber safety threats can concern for instance human errors and power supply issues that can lead to failure of a system. The cyber security threat consists amongst others of cybercrime by non-state actors[53] and cyber warfare and surveillance by governments.[54]

It is important to note that I study the contribution of university, government and industry to cybersecurity information diffusion. Hence, the study will focus primarily on the law and economics regarding the stimulation of cybersecurity information diffusion in an economic environment in which sufficient incentives for actors to do so are missing. Section 1.5 and Chapter 2, Section 2.2 will further introduce this part of the general framework of the study.

Naturally, there is only a problem of cyber security when there are threats in the first place, such as cybercrime. Hence, the cybersecurity information that ought to be diffused entails, amongst others, measures to reduce the impact of these threats. Thus, the cybercrime and cybersecurity markets are interrelated.[55] However, solely the

---

[52] Schneier (2003).
[53] For extensive threat overviews and descriptions, see Verizon's 2017 Data Breach Investigations Report <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/> (accessed on 30 March 2018); or the 2017 Symantec Internet Security Threat Report <https://www.symantec.com/security-center/threat-report> (accessed on 30 March 2018) or the various reports produced by the European Union Agency for Network and Information Security (ENISA): <Enisa.europa.eu/publications> (accessed on 30 March 2018).
[54] Cyberwarfare includes the use of cyberspace and targeting computers and networks in warfare. Mass surveillance is the surveillance of an entire or a substantial part of a population in order to monitor those people. Interestingly, information diffusion regarding cyberwar threats can also provide fruitful results as Stevenson and Prevost (2013) argue.
[55] Van Eeten and Bauer (2008), p. 16.

cybersecurity market is the subject of this study, with its focus on mechanisms that increase incentives for the stimulation of cybersecurity information diffusion. Accordingly, I will not study the motives and economic incentives of cybercriminals as such, nor will I give a detailed description, analysis and literature review regarding cybercrime. Instead, this section provides a brief overview of dynamics and development of cybercrime as part of the cyber security theatre.

Over the past years, there have been major developments in the dynamics of the cybercrime market. One of the main drivers for the development of this market is that with a decreasing amount of knowledge, a cybercriminal can execute increasingly more sophisticated attacks as Figure 2 shows.[56]. In the 90s, cybercrime was hard and did do little damage. In 2017 you can buy a botnet that distorts the computers of 1000s of people without any technical knowledge for just a few dollars

[56] Howard Lipson, Carnegie Mellon University (CMU) Software Engineering Institute CERT®

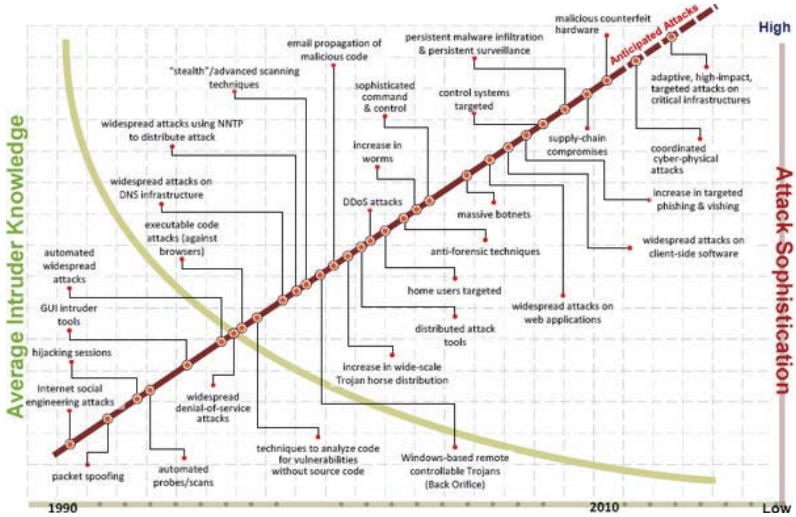


Figure 2: Average intruder knowledge versus attack sophistication over time.

The lower cost of operation combined with the higher potential benefits of cybercrime have led to increasingly more entrants to the cybercrime market.[57] In the past years, scholars observed that established cybercrime markets can be seen as common pool resources. Within these markets, the entry of more criminals results in less profits for the others.[58] Consequently, there is a strong incentive for cybercriminals to discover new cybercrime markets and exploit new vulnerabilities. This causes a 'red queen effect', whereby criminals and cyber defence systems are constantly adapting and innovating to be one step ahead of each other.[59] The red queen effect results in the

[57] See for instance <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> (accessed on 30 March 2018).

[58] Van Eeten and Bauer (2008); Moore and Clayton (2009).

[59] Edwards, Hofmeyr and Forrest (2016). The authors argue that the "Red Queen hypothesis in biology provides a possible explanation. It states that organisms not only compete within their own species to gain reproductive advantage, but they

temporal value of cyber security information. Solutions to mitigate these threats constantly emerge but get out-dated quickly.

1.3.3 Vulnerability

The above-discussed threat aims to exploit a weakness in a security system. Such a weakness is called a vulnerability. Vulnerabilities can be human or technical. Scholars estimate that up to 80% of exploited vulnerabilities are human. Humans are often the weakest link and by applying 'social engineering', a threat can often more easily penetrate a system.[60] Criminals often use large numbers to exploit a social vulnerability. An example is a phishing mail that is sent to 10,000 employees of a bank and whereby only 2 persons click on the link. Technical vulnerabilities are penetrable errors in first or third party security systems. A core concept is the 'zero day exploit', a vulnerability that has not been found yet by the owner or guardian of the computer program. In reality however, cybercriminals much more often exploit existing vulnerabilities, which are already known to the public, that have not been patched, which was also the case during the Wannacry and NotPetya attacks. The general dynamic here is that defending technical systems is much harder than attacking those systems. Suppose that a software product has a million lines of code, with 100 vulnerabilities.[61] And suppose a security expert can check 100 lines an hour. It will thus take 10,000 hours to discover and fix every vulnerability. However, a cybercriminal only has to discover one vulnerability before the security expert does discover it, which he can do in roughly 100 hours when he uses the same pace as the security expert. In this case, defending is roughly a factor 100 more time

---

must also compete with other species, leading to an evolutionary arms race." Also, Van Eeten and Bauer (2008) observe that the markets for cybercrime and cyber security are highly interdependent; See also Herr and Romanosky (2015).

[60] An example is 'CEO fraud', whereby the cybercriminal pretends to be the CEO.

[61] Anderson (2001) provided this example.

consuming than attacking. In practice, cybercriminals often use a combination of social engineering and exploiting vulnerabilities.

The example above shows that cyber security is an unbalanced game between defenders and attackers. There are a number of drivers that will likely increase this misbalance. First, the integration of existing systems through new technology increases vulnerabilities.[62] For instance, the integration of file management systems through cloud computing,[63] but also connection of new devices to the Internet known under the label of the Internet of Things.[64] Secondly, the political interest of governments in surveillance and cyber warfare blocks the necessary openness to fix zero day exploits and share information. For instance, the zero day that that formed the basis of the Wannacry and NotPetya attacks had already been discovered by the US National Security Agency (NSA). They did not disclose the vulnerability, to keep a back door for their own purposes.[65] Thirdly, software vendors can lack sufficient incentives to make good software products because they do not have to bear the cost of the errors these contain. However, it should be noted that software vendors have made an effort in mitigating this underpowered incentive by developing Software as a Service (SaaS) business models, which inherently have stronger

---

[62] This is also the cause of the systemic element of cyber risk, discussed in Section 1.3.5.

[63] Haas and Hofmann (2013).

[64] Examples are power plants information systems, which were separated from Internet until recently (Anderson (2009)). But due to new influences of technology such as the demand for 'smart meters' they are connected to the Internet on a large scale, which creates additional vulnerabilities (Suleiman et al. (2015), pp. 147-160).

[65] Perlroth and Sanger (2017) <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?mcubz=3> (accessed 30 March 2018); Hijink (2017) <https://www.nrc.nl/nieuws/2017/06/29/vernielzuchtig-cyberwapen-mede-dankzij-de-nsa-11334829-a1564924> (accessed 30 March 2018, Dutch).

incentives for vendors to maintain the security of their products, because they sell a service with a subscription instead of a product with a fixed price.

1.3.4 Impact

The impact is the damage to the assets of the computer system after the attack. The general dynamic is that the impact - the costs of cybercrime - has increased significantly over the past decades because of the increased number of cybercriminals that entered the market and the increased dependence of people on computer systems.[66] The following three breakdowns of impact will be used throughout the study.

1. *Personal data versus non-personal data.* Personal data can be related to individuals/persons. Examples are social security numbers, medical data and addresses.[67] Non-personal data is valuable information that cannot be related to natural persons, such as intellectual property or non-identifiable information of natural persons.[68] The fundamental right to the protection of personal data drives concrete data protection legislation. The crystallized data protection laws (hereafter: DPL) enable scrutiny with the law and economics methodology of the study. Personal data protection yields positive spill-over effects towards the protection of non-personal data. When personal data assets are better protected through for instance DBNLs, it

---

[66] Anderson, Barton, Boehme et al. (2013), pp. 265-300.

[67] Although breaches of personal data can occur on every medium, such as folders, CD-ROMs and analogue forms, nowadays, most personal data breaches that have significant impact are digital.

[68] See Pappalardo (2016) <https://www.lexology.com/library/detail.aspx?g=804ce9b8-dfa5-4c67-bbf7-4cc3e087c2f8> (accessed 30 March 2018).

is likely that overall resilience will improve.[69] Hence, personal data play a prominent role in the study. Part I and II exclusively focus on contributing to measuring the impact of personal data security legislation. Personal data is also considered a key insurable risk regarding the analysis on cyber insurance in Chapter 6.[70]

2. *First order damage versus second order damage.* First order damage equals the direct costs organizations incur when a cyber incident occurs. Organizations can lose personal or company data through hacking, or failing hardware and software or mistakes of employees can interrupt their business.[71] Second order damage is the negative effect of an incident once it becomes public,[72] such as reputation damage[73], fines of a DPA or liability claims. Hence, this distinction is relevant for Part II on DBNLs and Part III on risk shifting. The scope of second order damage is often more difficult to demarcate and estimate than first order damage. Therefore, there are particular complexities in shifting the risk of second order damage.[74]

3. *First party versus third party impact*. First party damage is damage at the organization that owns the information technology system.[75] Third party damage is damage at other

---

[69] Chapter 4 will extensively discuss the social benefits of data breach notification laws, for instance through 'the sunlight as disinfectant principle'.
[70] See for instance: ENISA (2012)
[71] Cebula and Young (2010) < https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395> (accessed 30 March 2018).
[72] Bandyopadhyay, Mookerjee and Rao (2004).
[73] Veltsos (2012), pp. 192-207
[74] This could result in suboptimal claim behaviour in the case of cyber insurance as I will discuss in Chapter 6.
[75] Schwarcz and Siegelman (2015).

organizations (or individuals) affected by the cyber incident. This is a relevant distinction for risk shifting in Part III, as for instance insurability is divided in first and third party risk. The distinction also plays a role in the discussion regarding DBNLs. As computer systems get more integrated into a network or a network of networks, the likelihood that third party damage will exceed first party damage will increase. The next section will address this further.

1.3.5 Cyber risk as a systemic risk

Section 1.3.1 to 1.3.4 illustrated that all three elements of cyber risk contribute to its overall surge.

1. More sophisticated threats at lower costs increases the likelihood of a threat.
2. The likelihood that the threat exploits a vulnerability has increased.
3. Impact becomes more significant as society is increasingly more dependent on the Internet.

So far, the discussion concerned the dynamics of an isolated cyber incident. However, the biggest elephant is still in the room: Cyber security incidents are (almost) never isolated. In other words, cyber security is a systemic risk. Systemic risk is not fully independent and correlates.[76] Stephen Catlin, the CEO of Catlin, warned in February 2015 that cyber risk present the 'biggest, most systemic risk' he has

[76] 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 (several subsets of) cyber risks, because such data is not available.

encountered in an insurance career of more than 40 years.[77] New systemic risks, which result from recent technological advancement, are a specific subset of those risks and cyber risk in itself a subset of new systemic risks.[78] The systemic element in cyber risk is caused by the high degree of interdependence between computer systems. For instance, when a cybercriminal wants to exploit a vulnerability in an operating system, he or she can do so at many computers. Hence the likelihood that a vulnerability in one system will be exploited correlates with the likelihood that another system will be exploited.[79] The fact that information technology is designed in a similar way and consequently is vulnerable to the same incidents can potentially result in catastrophic damage. In theory, there are cyber cases imaginable of perfect correlation, i.e. where all incidents occur simultaneously: a zero day exploit in a widely used operating system, a large-scale malware attack, or a vulnerability in a widely used operating system. We have seen this in the 2017 Wannacry and NotPetya attacks.[80] Nevertheless, there is little empirical evidence about the extent of correlation for various types of cyber risk. 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 occurred so far. Another feature of systemic risk is that incidents can have a large impact on third parties. This is called a cascade effect.[81] For instance, when an Internet Service Provider (ISP) is hit by a malware attack, this can have impact on its clients and other users of

[77] Gatlin is the owner of the largest syndicate at Lloyd's (Financial Times 5 February 2015).
[78] Faure and Hartlief; Ackerman (2013); World Economic Forum (2014).
[79] Baer and Parkinson (2007) doi:10.1109/MSP.2007.57 (accessed 30 March 2018).
[80] Although, also regarding these attacks, solely 3% of organizations that had that vulnerability were hit. Still, I would consider this as a large number since many organizations used the system that contained that vulnerability.
[81] Especially when critical points in the structure of the Internet are targeted, such as ISPs (Van Eeten et al. (2010)).

Internet traffic through this provider. Hence, correlated risk in an insurance portfolio is risk that simultaneously affects several insured parties. Cascade effects occur when the operationalization of one risk as such causes a domino effect at other third parties. These systemic elements of cyber risk makes investing in cyber security hard and likely to become harder in the future.

1.3.6 Investing in resilience

So far I have discussed the nature of cyber risk that can be divided in threat, vulnerability and impact. I also discussed the systemic element of cyber risk. In this section, I will discuss - very briefly - investing in cyber security, especially for those readers that are not very familiar with this subject. There is a vast amount of literature on the technicalities of investing in cyber security and I will refer to this literature for those who would like to dive deeper into this subject. A modern cyber security investment strategy often prioritizes the reduction of impact instead of reducing threats or vulnerabilities.[82] This strategy of 'robustness' and 'resilience' minimizes the risk of failure instead of minimizing the likelihood of the threat exploiting a vulnerability.[83] Failure means permanent damage to assets of the system. In robust and resilient systems incidents occur without causing damage or causing temporary damage (robustness) and the system can recover (resilience). As Bruce Schneier puts it: "The way to mitigate the risk of fraud due to impersonation is not to make personal information

[82] Some scholars have illustrated that optimal security does not necessarily have to be the primary concern of organizations, see Moore (2016).
[83] De Bruijne and Van Eeten (2007); Boin and Van Eeten (2013); Resilience is a relevant concept much beyond the protection of cyber risks.

difficult to steal, it's to make it difficult to use."[84] I will briefly discuss three interventions.[85] First, compartmentalization separates the components of the computer system, as a digital fire protection between several parts of the system.[86] Secondly, the implementation of diverse and independent layers of security mechanisms will make a system harder to penetrate. Last, back-ups are a simple though effective strategy especially when combined with encryption[87]. Encryption protects data confidentiality and integrity while back-ups protect data availability.[88] However, for some (and some say a large share of) organizations, a more sophisticated investment strategy is a second step in attaining optimal security. They must first implement the most basic security measures, such as the regular updating of firewalls, virus scanners and operating systems.[89] In practice, a cyber security strategy will first entail the listing of a variety of cyber security measures possible. After a prioritization process, the available budget will then be allocated among the most urgent measures.

1.3.7 Market power of software and security companies

Suppose an organization wants to invest in cyber security. It will shop for cyber security products in the market. In doing so, the organization will be confronted with another tenacious dynamic: the market power

---

[84] Schneier (2009) <https://www.schneier.com/essays/archives/2009/01/state_data_breach_no.html> (accessed 30 March 2018).
[85] See Anderson (2008).
[86] Pandya in Vacca (2014).
[87] Sometimes encryption can even serve as a safe harbour for organizations when complying with data protection laws. See Burdon, Reid and Low (2010).
[88] The so-called CIA triad is a useful framework for evaluating the protection of private communications (Arnbak and Van Eijk (2012); Pfleeger (2003) p. 504; Mulligan and Schneider (2013)).
[89] Crown (2015).

of software and security companies.[90] Relatively few players operating on the software and security market have significant market power. Their market power can be explained by the economics of information technology.[91] Goods[92] in information technology (and thus also security) are characterized by (extremely high) fixed costs and zero marginal costs. Hence, information technology goods usually have extreme economies of scale caused by these high fixed costs and network effects.[93] Examples are search engines, social networks and cloud services. Within these goods and services, 'the winner takes all' and natural monopolies are likely to emerge. Large companies exploit this market power by locking in individuals and organizations even further by increasing switching costs. Individuals and organizations have to outsource their information and security to big cloud services because they otherwise face high costs.[94] When these organizations are able to exploit their market power, this will lead to either under or overinvestment relative to the social optimum.

Section 1.3 discussed cyber risk, the drivers for cyber risk and provided a brief introduction into cyber security resilience strategies and the market power of the actors that provide security. This section concludes with stressing that the exact risk type and categorization is

---

[90] Market power is considered to be a source for market failure, see among others: Cooter and Ulen (2016), p 38.
[91] Varian and Shapiro (2004).
[92] This term is used in economic sense. The legal status of data and information and the question whether these are 'goods' in a legal sense is still the subject of much discussion.
[93] For instance, TOR network that works better when there is more traffic (Anderson and Moore (2007)).
[94] See Schneier (2012) <https://www.schneier.com/blog/archives/2012/12/feudal_sec.html> (accessed 30 March 2018).

of relatively little importance in the study because of the fast changing nature of the Internet. The analysis of incentives provides a better fundament for society and organizations to formulate of a sensible cyber security investment strategy. The main insight is that cyber incidents will occur and will continue to occur in the future. It is the very cyber security investment strategy regarding these incidents that determines the eventual organizational and societal cost of cyber security. The study aims to contribute to the information diffusion about the nature of cyber risk and the return on investment of strategies to reduce it. This means that, from a business operation perspective, cyber risk resilience can be achieved up to a private[95] adequate level where the marginal investments in resilience should equal the private marginal benefits thereof. This approach will not lead to perfect cyber security, but to the sensible security trade-off of optimal security in order to attain social welfare; the main topic of discussion of the next section. [96]

1.4. Cyber Security and Social Welfare

The study departs from the point of optimal security instead of perfect security. Whereas perfect security implicates zero cyber risk, an optimal security approach focuses on efficient risk reduction and consequently accepts an imperfect level of cyber security. The concept of optimal security is centralized in the notion of the study that sees cyber security investments as a means to enhance social welfare.[97] The goal of this utilitarian approach is to maximize social welfare through

---

[95] I define the private optimum as the business operation optimum of private parties,
i.e. individual organizations and consumers and not meaning the private sector.
[96] As Bruce Schneier points out in his book 'Beyond Fear' (2003).
[97] Economists usually assess states of the world by the criterion of social welfare, which ranks social states by the social welfare they attain (Bergson (1938), p. 310).

(allocative) efficiency.[98] Two definitions of efficiency, Pareto and Kaldor-Hicks efficiency, play a central role in law and economics. Pareto efficiency is usually defined as state of an allocation of resources where it is not possible to make one actor better off without making one actor worse off.[99] However, in most policy decisions, also in cyber security, it is unavoidable that some actors are left worse off to increase overall social welfare. This observation leads to the conclusion that Pareto efficiency is a difficult criterion for a more instrumental or pragmatic approach towards the improvement of legislation in cybersecurity.[100] Therefore, this study takes advantage of the alternative Kaldor-Hicks efficiency criterion, which state that it is allowed to leave actors worse off after a regulatory intervention, on the condition that winners of the intervention can possibly compensate those who are worse off.[101]

In economics terms, efficiency is commonly defined as the point where social marginal costs (SMC) equal social marginal benefits (SMB).[102] These marginal costs are the cyber security investments discussed in section 1.3.6. The benefits of reduced cyber insecurity exist in

---

[98] See (among many others) Posner (1973).

[99] See Cooter and Ulen (2016), p. 13. They define efficiency as follows: "A production process is said to be productively efficient if either of two conditions holds: 1. It is not possible to produce the same amount of output using a lower-cost combination of inputs, or
2. It is not possible to produce more output using the same combination of inputs."

[100] Calabresi (1991).

[101] Hicks (1939); Kaldor (1939).

[102] Posner (1972), pp. 29-96; Shavell (1980), pp. 1-25; Shavell (2004); Landes and Posner (1987); Cooter and Ulen (2004); Schäfer and Ott (2005); Shavell (1987); Brown (1973), pp. 323-350; Polinsky (1980), pp. 363-370; Faure (2009). See the following publications for an extensive discussion on this topic: Shavell (2004); Cooter and Ulen (2016). Schäfer and Ott (2005); Faure (2009).

decreasing cyber risk as discussed in section 1.3.1 through 1.3.4. The social welfare function is the aggregate of individual utilities. The optimized social welfare function can be described as the maximization of the sum of all private utility of individuals and organizations in society.[103] However, a 'laisser faire' strategy that strives for a maximization of private welfare in cyber security does not sum up to social welfare. In other words: there is a difference between private marginal cost and social marginal cost.[104] This is difference is caused by the externalities: the private benefits and costs of each individual actor are not isolated. On the contrary, the investment decision of each private entity is strongly related to other entities because of the systemic character of cyber security risk (1.3.2.). The systemic element of cyber security is the root cause of misaligned incentives and market failures, which I will discuss in Section 1.5. This section will first give a brief introduction into the social welfare perspective for assessing the cyber security landscape. The section will first introduce the contribution of the social welfare perspective (1.4.1) and its drawbacks (1.4.2). Subsequently, other perspectives relative to the social welfare perspective are discussed (1.4.3).

1.4.1 The contribution of a social welfare perspective

I will provide three contributions via the social welfare perspective. The first is that a social welfare function calculates total cyber security costs.[105] This means that not only the costs of cyber insecurity itself are

[103] The study mostly focuses mostly on organizations. It should be noted that there can be different aggregation mechanisms, for instance using the sum or the product of all individual utilities.
[104] Cooter and Ulen (2016), p. 39.
[105] Compare Calabresi (1970).

included, but also the cost of investing in cyber security.[106] Market power (Section 1.3.7) of organizations and agenda setting by governments could lead to insufficient attention for the cost of investing in cyber security and exaggerated attention for the cost of cyber insecurity. For instance, the cost of cyber security regulation, which could be considered a social investment in cyber security, is often neglected, as Part II on DBNLs will discuss.[107]

The second contribution is that the social welfare 'mind-set' relates marginal benefits and cost of cyber security to all other goods in the world. An allocative efficiency paradigm gives insight in the relative cost of cyber security. In the end, attaining social welfare is not only a question of investing in cyber security but part of a distribution of scarce goods that could also be allocated to other societal goals such as healthcare and education.

Thirdly, the social welfare perspective will provide awareness of the cost of the inefficiency of overinvestment in cyber security. There can be valid reasons to deviate from the most efficient investment level, for instance because we want to protect private communications and fundamental rights.

1.4.2 Pricing the social welfare function

The social welfare function necessitates pricing costs and benefits of cyber security investments and insecurity. Sometimes, the impact on

---

[106] See also Anderson (2008), p. 816: "The first killer problem is understanding the trade-off between risk and reward. Security people naturally focus too much on the former and neglect the latter."

[107] See part II where I will extensively discuss the data breach notification law. This part will show that the design of DBNLs can lead to a net social loss when the threshold for notification is set too low.

the economy of cyber incidents can be quantified, such as the discontinuity of organizational activities. For instance, the total costs of the NotPetya attack exceed €100 million.[108] Likewise, the cost of other tangible assets can be determined up to a reasonably accurate level, such as the value of getting a fine from a data breach notification authority.[109] However, much more often, pricing damage is hindered by information asymmetry, unavailability, incorrectness and temporality.[110]

So far, I still only considered price determination ex post (after the event did materialize), which is relatively straightforward. It is even harder to determine the likelihood of a threat taking place and the likelihood of the threat exploiting vulnerability.[111] Up until now I discussed pricing of economic damage. The pricing complexity increases even further when values enter a range that complicates accurate inclusion in an economic framework. One could for instance think about privacy infringements. In such a situation, the economic framework does not fit, because consumers sell their privacy below their initial willingness to accept. Hence, this behaviour confounds the objective determination of their value of privacy.[112] The problem is

---

[108] Ricadela (2017) <https://www.bloomberg.com/news/articles/2017-08-03/europe-s-cyber-victims-racking-up-hundreds-of-millions-in-costs> (accessed on 30 March 2018).

[109] This issue will be discussed further in part II, whereby the expected value of the fine by the DPA is one of the key drivers of (non-)compliance with the data breach notification law.

[110] See Section 1.5.2

[111] See among others Anderson et al.: The difficulty of determining the likelihood and impact of cyber security threats is one of the reasons that the cyber insurance market does develop slowly (2012). Part III will extensively discuss this market and will provide a risk shifting solution that exactly works around the issue of ex ante determination of risk, called cyber risk pooling.

[112] Cofone (2015), chapter 3.

aggravated by the fact that non-tangible assets often are traded off against more tangible assets. This for instance concerns the 'trade' of privacy for more security.[113] Another issue that exacerbates the pricing problem, is that utility preferences differ largely over people with often different agenda's in the cyber security game. Hence, one needs to take into account each individual preference regarding cyber security and privacy.

The discussion above has demonstrated that pricing cyber security is hard or even impossible because of the hampered determination of probabilities, non-economic impact and individual utility preferences. The question remains in what way the social welfare perspective can contribute to put the cyber security puzzle together. The focus of the study utilizes the potential of social welfare while circumventing the difficulties in pricing the social welfare function. This is caused by the studies' focus, that will lie on means reduce information asymmetry and stimulate information diffusion in cyber security. Information diffusion is likely to increase private optima because it allows for better-informed choices of organizations.[114] Information diffusion also decreases transaction costs and in doing so it can reduce the misaligned incentives caused by for instance externalities.[115] Without a doubt, increasing information diffusion in itself also has a cost, and this should be balanced with the benefits thereof. For instance, Part II will balance the costs of a data breach notification law with its benefits in increasing the diffusion of information in the cyber security market.

---

[113] See for instance Pavone and Esposti (2010).
[114] Klick and Parisi (2004).
[115] Externalities are discussed in Section 1.5.1 and information diffusion as such in Chapter 2, Section 2.2.

1.4.3 Other criteria for the distribution of cyber security investments

The social welfare perspective of the study has a set of neoclassical criteria and concepts that facilitate the determination of the optimal distribution of cyber security investments, namely utility maximization, efficiency and rationality. I have discussed some of the challenges within the perspective relevant for the study, such as the difficulties in determining utility and subsequently pricing it (1.4.2.). The focus on stimulating knowledge diffusion mitigates or circumvents some of these challenges. However, the focus of the study does not circumvent the existence of other possible sets of criteria to distribute cyber security investments.[116] I will discuss fundamental rights protection and the techfix because they drive the policy debate in cyber security and could lead to overinvestment in cyber security relative to the social optimum.[117]

Fundamental rights protection within cyber security states that the fundamental right to privacy and private communications means that cyber security and privacy should be attained at all cost, also when this entails a level of protection that is not efficient. Their fundamentality is non-negotiable. For instance, some legal scholars advocate the protection of private communications as 'a first line of defence'.[118] The implication is that privacy should therefore be prioritized over efficiency and other fundamental rights.

---

[116] See Mulligan and Schneider (2011) for several doctrines related to cyber security.

[117] There are also other more traditional criteria in law and economics, such as fairness, happiness and market outcomes (Renda (2011)) and see also for an interesting discussion Bozeman (2007). The utilitarian approach has been criticized in the literature of the past century (Sanchirico (2001), pp. 1003-1089).

[118] Arnbak (2015).

The techfix is the belief that cyber risk can be reduced to (almost) zero by technical solutions. Given the discussion about the nature of cyber risk and its inherent instability it is hard to provide an argument for the techfix being a realistic solution. However, in practice, there are factors, such as information incorrectness, agenda setting and intolerance for ambiguity, that lead to increased incentives to campaign for a techfix. This causes overinvestment in cyber security. Sometimes, the techfix serves a legitimate goal, for instance by serving fairness or fundamental rights. It can also drive new technical solutions. In such a situation, the techfix approach is a means to an end, but still quite often it is framed as an end in itself by actors in the 'security theatre' that make false promises.[119]

It is not my goal to claim that maximizing utility is the only legitimate end. Especially the fundamental rights perspective can be equally relevant as the efficiency criterion adhered in the study. However, one of the virtues of the efficiency criterion is that it can provide an indication of the costs of fundamental rights and techfix approach relative to the most efficient outcome. For instance, increased investments in private communication (in order to protect fundamental rights) could reduce national security (targeted surveillance) or increase the (administrative) costs faced by businesses and individuals. It could even reduce aggregate social welfare. The latter may be traded for private communications protection. But to make informed policy choices, one must be cognisant of the utility yielded by each legal instrument.

[119] Schneier (2013) for instance describes this 'security theatre', which are measures designed to get a feeling of security rather than having real impact.

1.5. Misaligned Incentives

Section 1.3 discussed the dynamics of investing in cyber security and Section 1.4 discussed the societal perspective of investing in cyber security. The study already discussed that the attainment of private optima is not going to lead to efficiency. 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.[120] Cyber risk is a systemic risk. Because of the interconnectedness of computer systems, private investments have a positive of negative effect on third parties. Micro-economics labels this phenomenon as an 'externality', a type of market failure.[121] Externalities give rise to misaligned incentives of organizations that hamper their contribution to maximizing social welfare.[122] They either invest too much or too little in cyber security. This section will give a brief introduction in the roots of these misaligned incentives and its relevance for the specific approach of the study. The analysis of incentives lies at the core of the field of economics of cyber security that emerged in the early 2000s. A group of research scholars proposed that cyber security is not a question of technology only, it is also and possibly more a question of correcting microeconomic incentives, and the economics of cyber security emerged.[123] The analysis of incentives is also key in law and economics. As already illustrated, the integration of law and economics with these economics of cyber security is the third ambition of the study. The externalities and related public good characteristics of cyber security will be discussed in Section 1.5.1. Section 1.5.2 illustrates four types of information deficits as a prelude to Chapter 2.

---

[120] Majuca, Yurcik and Kesan (2006) <http://arxiv.org/abs/cs/0601020> (accessed 30 March 2018).

[121] Stiglitz (1989); Bator (1958); Posner (2007), p.72

[122] Varian (2010); Cooter and Ulen (2016).

[123] See also Section 1.2; the seminal article by Anderson (2001) and for a good overview, Bauer and Latzer (2016).

These deficits are also related to externalities that cause the underproduction and underdiffusion of information being one of the main building blocks of the specific scope of the study.

1.5.1 Externalities and public good characteristics

Negative externalities exist when the activity of a first party causes a cost towards a third party. The party has an incentive to overinvest because the first party does not have to bear the third party costs. In general, cybercrime causes disproportionate cost on society and cybercriminals are sometimes referred to as 'metal thieves', in the sense that the societal damage caused is much larger than the private gains of the criminal.[124] In the 2017 NotPetya attack, the cybercriminals received around $10,000 in bitcoins[125], while the total costs of the NotPetya attack exceed €100 million.[126] In general, cyber security investments benefit others and generate positive externalities instead of negative externalities.

Positive externalities exist when the activity of a first party causes a benefit towards a third party and thus the party investing does not take the full benefit of its decision.[127] Hence positive externalities give

---

[124] Anderson et al. (2012).

[125] Graham (2017) <https://www.cnbc.com/2017/06/28/ransomware-cyberattack-petya-bitcoin-payment.html> (accessed 30 March 2018); Spring (2017) <https://threatpost.com/google-study-quantifies-ransomware-revenue/127057/> (accessed 30 March 2018); Hern (2017) <https://www.theguardian.com/technology/2017/jul/05/notpetya-ransomware-hackers-ukraine-bitcoin-ransom-wallet-motives> (accessed 30 March 2018).

[126] Ricadela (2017) <https://www.bloomberg.com/news/articles/2017-08-03/europe-s-cyber-victims-racking-up-hundreds-of-millions-in-costs> (accessed 30 March 2018).

[127] The analysis of externalities in cyber security is an extensively discussed topic. The literature is too vast to mention in its entirety, so I shall limit myself to

incentives to underinvest. Individual private investments in cyber security usually benefit societal cyber security. For instance, when a computer system of an organization is infected by malicious software that secretly makes them a part of botnet, its systems will be used to execute (large scale) attacks on other systems.[128] However, it is in the interest of the botnet owner to let the attacks go unnoticed so that the owner of the system will not remove the malicious code. The owner of the infected computer system thus feels no nuisance of the botnet system. Hence, the benefits of removal of this software are on society, that will experience, ceteris paribus, fewer botnet attacks, while the private owner of the system mostly incurs costs of detection and removal of the malicious code and few benefits. This imposes a problem on society, because there will be no incentive for the private owner to remove malicious code present on its systems or even install programs or do an effort to detect them in the first place. The owner of the system has an incentive to underinvest relative to the social optimum. This could lead to a situation where every organization will anticipate on the actions of third parties that will provide security. In such a situation, these positive externalities lead to no investment at all; the so-called free rider problem. For instance, society would greatly benefit from openness and information exchange about zero-day exploits. But such openness often does not benefit the party that gives openness in the short term. Instead, those parties may choose to free-ride on other parties providing information for them.[129]

---

mentioning a few key articles: Moore (2010); Anderson (2001); Anderson and Moore (2007); Anderson (2001), chapter 7; Bauer and van Eeten (2009).

[128] Asghari, Bauer, Tabatabaie et al. (2010)

[129] Powell (2005). A second common potential market failure in cybersecurity documented in the economics literature deals with the problem of information sharing and free riding. A number of papers explore this. Anderson (2001) looks at

The pervasive existence of positive externalities in cyber security has led to the discussion whether cyber security can be seen as a public good.[130] A public good has the two following closely related characteristics:[131]

- Non-rivalrous in the sense that consumption by one individual does not reduce consumption opportunities for other individuals.
- Non-excludable in the sense that everyone can freely consume the good

For instance, national defence or fresh air are considered as pure public good.[132] The consumption of national defence or fresh air of a consumer does not reduce the consumption of others and everybody can freely consume it. It becomes quite clear that, based on this definition, cyber security is not a (full) public good because for instance an IT environment can be excluded from the public environment through firewalls, honeypots and other intrusion detection and prevention systems. However, the systemic character of cyber risk (see Section 1.2.3.) is not excludable. Everybody enters the global Internet but is in different ways vulnerable for several types of hazards depending on the browser they surf with, the operating system they use and the protection they invested in. Vulnerabilities in Android, iOS

---

the incentives facing information sharers, Varian (2002) models the free rider problem and system reliability, Gordon
et al. (2002) look at information sharing by SB/ISOs, Gordon et al. (2003) study the welfare implications of information sharing and the conditions necessary for information sharing to increase computer security, and Schechter and Smith (2003) examine the benefits of sharing information to prevent security breaches.

[130] Cooter and Ulen (2016).

[131] Varian (2005).

[132] Cooter and Ulen (2016).

or Windows affect large parts of cyber space. Patching them has close to zero marginal production costs when everybody can freely download the patch and most software companies do not exclude consumers from using such a patch. Thus, most scholars agree that cyber security has the *characteristics* of a public good. The degree to which cyber security is a public good depends on the intensity of positive externalities. When externalities are relatively limited (private benefits are high and public benefits are relatively low) there will be sufficient private incentives to provide for security. For instance, when a company, such as a bank, has a high interest in keeping trust in its digital services, private benefits are high and likewise there will be incentives to provide for security.[133] The literature on public goods is of value to the study, because it provides necessary conditions and solutions regarding ensuring the production of public goods and avoiding the tragedy of the commons.

1.5.2 Information deficits

Misaligned incentives, public good characteristics, but also the existence of market power at software and security firms[134] and the capricious nature of cyber risk[135] lead to information deficits in the cyber security market. There is a lack of reliable data about cyber risk and a lack of information about the return on cyber security investments.[136] As said, one of the main overarching goals of the study

---

[133] Powell (2001) <http://www.independent.org/pdf/working_papers/57_cyber.pdf> (accessed 30 March 2018); these private benefits have for instance led to a quite spectacular decrease in the cost of Internet banking fraud since banks had sufficient incentives to take appropriate measures to mitigate the vulnerabilities.

[134] See Section 1.3.7.

[135] See Section 1.3.

[136] See for instance Anderson (2001), but also in relation to the insurability of cyber risks by Böhme and Schwartz (2010); Biener, Eling and Wirfs (2015); Eling and Schnell (2016).

is to contribute to the reduction of these deficits. I will pursue this goal by focusing on the university-government-industry helix and their role and possibilities in stimulating information diffusion. But before introducing the specific focus of the study in the next chapter, I will first discuss four general information deficits in cyber security: unavailability, asymmetry, temporality and incorrectness.

1. *Information unavailability.* An information deficit can exist in the fact that cyber security information is simply not available. When an organization has no intrusion detection system or a simple virus scanner it will receive no or little information about threats, vulnerabilities and impact. Information unavailability mostly results from the externality problem. Recall the positive externalities in cyber security: Organizations have insufficient incentives to investigate what is going on because the cost of their potential cyber insecurity is being borne by others. Another possible reason is that the organization is simply not aware of the costs associated with the cyber risk and therefore does not collect risk metrics at its computer system.

2. *Information asymmetry.* When information problems in cyber security are analysed, the discussion focuses often on problems related to information asymmetry.[137] In a situation of asymmetrical information, one actor or a group of actors possess a certain piece of information while another actor or group of actors does not. Hence, sellers do know more about the quality of the goods than buyers or vice versa. For instance, information asymmetries exist for organizations purchasing

[137] Cooter and Ulen (2016), p, 41.

products to reduce cyber risk, because it is difficult for them to assess the quality of Internet security products.[138] Both market power and externalities drive asymmetrical information in cyber security. Market power concentrates the resources available for obtaining information in the first place.[139] The organizations' incentive to share information is misaligned in the sense that it does not benefit from sharing this information. In such a situation, the public good characteristic of cyber security emerges.

3. *Information temporality.* The lack of information is caused by the fact that the type and impact of cyber threats change continuously and it is hard or impossible to forecast impact based on past data. Section 1.3.2 showed that cybercriminals have strong incentives to find new exploits for vulnerabilities to escape their own tragedy of the commons. They usually enter fruitful ground since software and security companies continuously develop new products that contain new vulnerabilities. Also the further integration and stacking of computer systems generate additional vulnerabilities. Hence the value of historical data about cyber risk depreciates with an increasingly fast pace. It has even less predictive power for the future.[140] For example, only in recent years, cyber security

[138] Moore (2010), pp. 103-117.
[139] Chapter 2, Section 2.2 will relate the four types of information deficits to the three stage of the cyber security information value chain.
[140] Chapter 6 discusses that this is especially an issue for cyber insurance companies when trying the calculate premiums based on actuarial data.

experts observed a giant spike of ransomware.[141] Ransomware is a malicious piece of software that takes a computer 'hostage', in the sense that the owner cannot access the computer before a certain kind of ransom is paid, mostly in the form of a digital currency such as bitcoin. This contrasts with Internet banking fraud, which declined sharply in the Netherlands after banks took effective security measures and is not really an issue anymore.[142] Thus, long-term data about the frequency of occurrence and average damage is unknown. Consequently, parties have difficulties in determining the right security measures.

4. *Information incorrectness.* Obviously, information can become incorrect when it has become outdated as a consequence of the above-mentioned temporality. In that sense, there is an overlap between information temporality and incorrectness. However, there are also incentives of security and software companies for an intended overestimation of the cost and severity of cyber security, because they have a benefit in selling security products.[143] In many occasions, this information is not strictly

---

[141] See for instance Hern (2016) <https://www.theguardian.com/technology/2016/aug/03/ransomware-threat-on-the-rise-as-40-of-businesses-attacked> (accessed 30 March 2018).
[142] Total damage of Internet banking fraud in the Netherlands declined sharply from €4,7 million in 2014, €3,7 million in 2015 towards €148,000 in the first half of 2016. This contrast with the figures that were measured when Internet Banking Fraud was at its height of its impact, the first half of 2012, there was €24,7 million damage. See <https://www.nvb.nl/veelgestelde-vragen/veiligheid-fraude/1816/hoe-hoog-is-de-schade-door-fraude-met-Internetbankieren.html; https://www.nvb.nl/thema-s/veiligheid-fraude/586/fraude.html; https://fd.nl/economie-politiek/1167515/fraude-met-Internetbanken-spectaculair-gedaald> (accessed 30 March 2018).
[143] Anderson et al. (2012).

incorrect, but just a biased collection and aggregation of the available data. For instance, cyber security reports overestimate the direct costs of cybercrime.[144] Organizations and individuals that make investment decisions can also unintendedly overestimate the costs of cyber security, for instance as a consequence of behavioural biases. For instance, organizations perceive the reputational impact of data breach disclosure as very high while the long term impact of these breaches on for instance stock market value has never been demonstrated.[145] The issue is aggravated by the fact that there are very few academic studies that measure the cost of cybercrime, and thus objective information is scarce.[146]

Section 1.5.2 briefly identified the several information deficits and related them to microeconomic theory. It is exactly this theory that provides instruments beneficial to the identification of solutions for overcoming these deficits throughout the study. For instance, the cyber risk pool discussed in Part III uses the literature on public goods. Instead of being public, cyber risk pools act as private information-sharing groups that can exclude non-members. The incentives for sharing information could improve when there is an ability to exclude members suspected of holding back information, as I will show in Part III.[147]

---

[144] Florêncio and Herley (2012) <http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?mcubz=3> (accessed 30 March 2018).
[145] Compare for instance Goel and Shawky (2009), pp. 404-410
[146] Among the few studies that did try to quantify the cost of cybercrime is Anderson (2012).
[147] Tullock (1985); Powell (2001) <http://www.independent.org/pdf/working_papers/57_cyber.pdf> (accessed 30 March 2018).

1.6. Summary

This first introductory chapter has discussed the methodology and procedural strategy of the study, the general dynamics of investing in cyber security, the social welfare perspective and the bottlenecks of attaining this perspective. As we have read, the technical nature of cyber security risk is capricious due to its systemic element and its inherent advantage for attackers. The difficulty of finding adequate solutions is even aggravated by several microeconomic bottlenecks. This chapter introduced the reader to the general cyber security theatre. Against this background, Chapter 2 will introduce the specific research agenda that aims to contribute to improving this environment.

2. INFORMATION DIFFUSION AND THE TRIPLE HELIX

2.1. Introduction

The previous chapter illustrated that individual cyber risk is not a local phenomenon such as for instance fire risk, but instead correlates with the risk of other digital devices in the world. This affects the dynamics of the microeconomic theory explaining cyber security. One could say that microeconomic theory in cyber security is 'on steroids': the interwovenness of digital devices amplifies misaligned incentives, information deficits and other market failures. Where the previous chapter introduced the technical and economic challenges of cyber security, this chapter will introduce three lines of thought for solutions, namely information diffusion, legal instruments and the triple helix approach.

Section 2.2 starts with a discussion of the concept of information diffusion as a stage in the information value chain. Information diffusion will be related to the various information deficits that were introduced in the previous chapter. Section 2.3 introduces the legal instrument as the main medium the study will investigate. Section 2.4 will introduce the triple helix approach; the doctrine that university, government and industry all have their own role, tools and responsibility. Finally, after the theoretical framework has been established, Section 2.5 will introduce the specific issues that are the subject of the studies' three substantive parts.

2.2. Information Diffusion

Information diffusion[148] is the continuous circulation of information (in Part I related to the nature of DPLs and in Part II and III related to the return on cyber security investments and the nature of cyber security risk).[149] This section will explain the concept of information diffusion as part of the information value chain. Next, the benefits and costs of information diffusion will be discussed.

2.2.1 The information value chain

Table 3 below displays the three steps of a comprehensible information value chain I would like to outline here.[150]

Table 3: The information value chain

Part of the value chain	Contribution to the information deficits described in Section 1.5.2.
Step 1: creation	Unavailability; incorrectness
Step 2: diffusion	Primarily: asymmetry, Secondary: incorrectness; temporality
Step 3: utilization	Indirectly through the utilization of means for creation and diffusion

Creation. Logically, cyber security information needs to be created in the first place before it can diffuse among actors. Chapter 1 illustrated

---

[148] I use the economic definition of information diffusion. This is different from for instance the information theory of Shannon Weaver.

[149] See Chapter 1, Section 1.3.

[150] See Rogers (1962); Abelson and Glaser (1983; Rich (1979). This research distinguished the three processes of what I call, the information value chain, but it should be noted that this stream of literature mostly focused on innovations (rather than best practices) and scientific research (rather than organizational measures). Also, instead of information the word 'creation', one could also use the word 'registration'.

the current underproduction of information due to its positive externalities.[151] But still, information creation has private benefits. An example of information creation is the installation of a virus scanner that detects malicious software. In doing so, the information created directly reduces private cyber risk because the owner knows when malicious activity occurs. But, he retrieves information from just a small part of the cyber security landscape. Apart from reducing information unavailability, information creation can also reduce information incorrectness, in a situation where the correct information was not available but parties spread incorrect information to (deliberately) distort the market. Information creation will not be the main theme of the study. It is the field of the economics of cyber security that contributes to cyber security information availability.[152]

Diffusion. Information diffusion theory describes a wide range of events such as adoption rate of innovations, the disseminations of news and network effects of social media.[153] Information diffusion primarily reduces information asymmetry. As a second order effect it can contribute to a reduction of information incorrectness and temporality but the study will focus on its contribution to the reduction of information asymmetry.

The nature of information diffusion differs between Part I on the one hand and Part II and III on the other. This study focuses on the circulation of information regarding the nature of 71 DPLs in Part I by coding these laws. In doing so, it contributes to the reduction of information asymmetry. The information regarding these laws was

---

[151] See Chapter 1, Section 1.5.2.
[152] Key scholars in the economics of cyber security have urged for the wider availability of empirical data. See for instance Anderson et al. (2008)
[153] Wu, Chen, Xian et al. (2016).

already existent, but the quantification allows for easy access and comparison between laws by policy makers and other researchers. As a secondary effect, it can reduce information incorrectness about these laws, because the correct information is more easily accessible after the analysis.

Part II and III focus on information related to the return on cyber security investment and the nature of cyber risk. This means that private parties share their knowledge with other parties.[154] Contrary to the private benefits of the creation of information, the benefits of sharing information are almost solely external. Also here, information diffusion primarily reduces information asymmetry asymmetry. Secondary, when the correct information is being diffused continuously, it also mitigate the issue of information temporality and incorrectness.

There are very limited private benefits of information sharing. In a free market environment, the only private benefit a party gains is the likelihood of the reciprocity (the other party also shares its information) and appropriateness (it is morally good to contribute to society).[155] Moreover, information sharing is constrained by privacy issues or sensitive/competitive data related to business operation.[156] Thus, in many cases, there are insufficient incentives to diffuse

---

[154] Cyber security information diffusion is regarded as an important matter. See for instance Fuentes, González-Manzano, Tapiador et al. (2017), p. 127, which state: "Cooperative cyberdefense has been recognized as an essential strategy to fight against cyberattacks. Cybersecurity Information Sharing (CIS), especially about threats and incidents, is a key aspect in this regard."

[155] Ayres and Braithwaite (1992).

[156] See for instance Chapter 4. The GDPR constrains the processing and sharing of personal data.

information and to reduce asymmetry. This leads to the conclusion that information diffusion has very strong public good characteristics.[157]

Utilization. Information creation and diffusion solely contributes to social welfare when the information is utilized to make efficient cyber security investments.[158] In fact, in many information value chain theories, this is not a single step, but a process of several steps.[159] Utilization of information can also lead to the creation and diffusion of new information (for instance when an organization based on better information related to cyber risk invest in a monitoring and detection system.) In that sense, the information value chain is an iterative feedback loop. The specific methods on how to utilize cyber security information will not be included in the scope of the study. These matters of the technical execution in cyber security are especially debated within the domain of computer science.

2.2.2 The social benefit of information diffusion

Information diffusion results in more efficient cyber security investments and an increase in social welfare. The most simple and straightforward argument is that organizations do not have to 'reinvent the wheel'. Parties can learn from the experiences of other

---

[157] For the general discussion on public good characteristics of cyber security, see Chapter 1, Section 1.5.1.

[158] Here a challenge arises that, when information creation and diffusion increases, it is even more important to filter relevant data, as also observed by Zhang, Lui, Zhan et al (2016), p. 28. Ideally, this filtering stage already takes place at the diffuser of the information. This matter is also addressed in the light of data breach notification laws in Chapter 4.

[159] The field of knowledge management has provided useful insights in this area, see for instance: Serban and Luan (2002), who speak of data, information, knowledge and decision making.

parties in making efficient cyber security investments.[160] Insofar the costs of reinventing the wheel are higher than the costs of diffusing the best and worst practices this could lead to a social welfare surplus. Perhaps, it may seem obvious that reinventing the wheel is a more costly exercise than learning from others. However, there is certainly a perceived barrier to use others' information, especially when it is not diffused in a proper manner, and this causes that still many individuals and organizations first try to fix issues themselves. Secondly, the diffusion of cyber security data will lead to better informed people[161] and better products, such as cyber insurance. The cyber insurance market benefits from an increased availability of data because this allows for better premium determination.[162] Cyber insurance can in itself contribute to the diffusion of information through, for instance the aggregation of claim data. Hence, in a well functioning cyber insurance market a positive feedback loop will emerge that propels information diffusion.[163] Thirdly, information diffusion balances market power of big software and security firms, which have fewer possibilities for exploiting information asymmetries. They sometimes do so by releasing exaggerated cyber security statistics with information about threats, vulnerability, impact and resilience strategies.[164] Organizations can purchase a better-fitted product when the information asymmetry between the seller and the buyer (a lemon market) is reduced. When the uncertainty regarding the return on

---

[160] See for instance Anderson (2009) and its recommendations for the Internal market: On recommendations is: "We recommend that the EU adopt a combination of early responsible vulnerability disclosure and vendor liability for unpatched software to speed the patch-development cycle."
[161] Sohrabi Safa and Von Solms (2016).
[162] See Chapter 6.
[163] See Chapter 6.
[164] Anderson, Böhme, Clayton et al. (2008).

investment of investment in cybersecurity decreases, also the option to defer the investment decision decreases.[165] Fourthly, the classic law and economics argument is that when information diffusion reduces transaction costs, this could lead to a reduction of the externality problem.[166] It is important to note here that it is the diffuser of information that can lower transaction costs for the recipient of information. For instance, when an organization puts a cyber security best practice on the Internet, it will lower transaction costs for others to find and utilize this best practice.[167] The Coase theorem states that in a situation of zero transaction costs, parties will bargain up until efficiency has been reached. For instance, when a ransomware attack occurs, other parties can bargain with the affected party to not pay the ransom because the other parties have the benefit of lowering their own chances of being affected by ransomware. Naturally, the existence of zero transaction costs is just an ideal situation that will not be reached in real life, as Coase himself also observes.[168] Nonetheless, the less strict Coase theorem says that legal instruments should aim at reducing transaction costs. It should be noted that the interconnectedness of IT systems makes the concrete bargaining process complex or in some situations almost impossible because simply too many people are affected.[169] So 'Coasian bargaining' could emerge in smaller pools, such as the risk and insurance pools that are

---

[165] Gordon, Loeb, Lucyshyn et al. (2015).

[166] And legal instruments should be aimed at reducing transaction costs according to the positive school of L&E and the Coase theorem (Renda (2011); Posner in Parisi and Rowley (2005); Parisi (2004));

[167] Zhang, Liu, Zhan et al (2016).

[168] Coase (1960); see also Nagurney and Shukla (2017) who reach similar conclusions with regard to information sharing in cyber security and prefer a Nash bargaining model for cooperation and knowledge sharing to a Nash equilibrium model for non-cooperation.

[169] Or at least it will demand an efficient globalised bargaining system.

studies in Part III. Legal instruments can provide incentives to reduce these transaction costs.

2.2.3 The social cost of information diffusion

Apart from a social benefit, the stimulation of information diffusion also leads to societal costs, which should be balanced with its benefits. In the first place, the stimulation of information diffusion could lead to an underproduction of information creation by the party who expect to receive the information. In other words: when everybody expects the other party to diffuse information, there is no information created in the first place. Secondly, the stimulation of information diffusion could also lead to an underproduction of information by the party who created and registered the information in the first place, provided that the diffusion of information has a negative effect on the first party (and a positive externality on third parties). An example of this situation discussed in the study is the incentive not to detect data breaches when data breach disclosure is mandatory.[170] In such a situation, the diffusion of information has possible negative effects on the organization because of the administrative and reputational costs involved in its mandatory disclosure. Thirdly, some say that the protection of information internalizes the positive externality to third parties. This is the general argument in the discussion related to the social outcomes of the protection of patent law. However, in general, in order for information to be protected under patent law, this information should be new, sufficiently distinguishable from other inventions and universally applicable.[171] It becomes clear that the

---

[170] And Polinsky and Shavell (2006). See also Chapter 4, Section 4.6.1.

[171] See for instance European Patent Convention) of 5 October 1973 that formed the basis for European patent policy. The alternative, copyright law, is of less relevance since this mainly concerns creative content and not the application of a technical novelty.

majority of best practices related to cyber security do not fall within this scope and hence are not patentable. Likewise, what is meant by information diffusion in this study does not include patentable innovations by cyber security or software companies. Instead, the focus of the study lies on information diffusion about non-patentable cyber security best practices and to avoid reinventing the wheel.[172] Finally, the public good nature of information diffusion with its free rider character necessitates the construction of additional structures that incentivize organizations to diffuse information. The costs of these incentive structures need to be less than their benefits. The practical execution of information diffusion is the subject of the next section.

2.2.4 The practice of information diffusion

Certainly not everybody does free ride on (the expectation of) information diffusion in cyber security. In 2015, Moore, Scott and Chang interviewed 40 Chief Information Security Officers (CISOs) from large (mainly US) companies and identified that there is "a good deal of information sharing in cyber security", for instance through Information Sharing and Analysis Centres (ISACs) and more informal CISO talking shops.[173] On the other hand, the Dutch cyber security council, with members from university, government and industry, has emphasised that the lack of information diffusion is one of crucial

[172] However, one should be aware that underproduction of information is also connected to the field of data protection. Insufficient personal data protection could also lead to an underproduction of information. However, most crucial information related to cyber security diffusion can be shared without disclosing details about natural persons. The relevant information will be more in the sphere of the nature of the risk and strategies to reduce it at affordable cost, which can even contribute to personal data protection. See Cofone (2017).
[173] Moore (2015).

bottlenecks in cyber security.[174] Quite naturally, large organizations have many resources at their disposal to engage in the information diffusion activities. Therefore, this study takes into account the information diffusion potential for somewhat smaller organizations. For instance, Chapter 6 empirically analyses the cyber insurance market for small and medium enterprises (hereafter: SMEs). These organizations often do not have separate CISO functions and cannot take part in the labour intensive ISACs. For organizations, and these kinds of smaller companies in particular, it is crucial to be able to engage in information diffusion at relatively low cost.

With regard to this low-threshold information diffusion, it is promising to note that the costs of the execution could eventually become low, provided that the right techniques are developed to provide valuable information to the right persons.[175] The technical execution of sharing information could be straightforward due to the low marginal cost of products in information technology industries. This gives rise to the promise that there is indeed low hanging fruit. However, while some parts of information diffusion arguably can be automated, some social innovation and best practices diffuse better when exchanged from peer to peer on an informal level and some ways of information diffusion require certain expert knowledge of for instance the legal system as Chapter 3 will show. But before the practical execution of information comes into play, the incentives of organizations to do so must be aligned. Consequently, this study does not focus that much on the practical effectuation of information diffusion (apart from Chapter 3), but rather studies techniques to

---

[174] Cyber Security Council (2017) <https://www.cybersecurityraad.nl/binaries/CSR-advies%202017%20nr.%202%20-%20Naar%20een%20landelijk%20dekkend%20stelsel%20van%20informatieknooppunten_tcm56-269317.pdf> (accessed 30 March 2018).
[175] Cetin, Gañán, Korczynski et al. (2017).

intensify the incentives of organizations to engage in information diffusion. The tool to align this incentive is the legal instrument, the subject of the next section.

2.3. Focus on Legal Instruments

The study focuses on the role of legal instruments in contributing to information diffusion and social welfare.[176] These legal instruments can fall within the scope of public or private law. The study addresses both legal areas. Within public law, the focus lies on (administrative) cyber security regulation, more specifically DPL (Part I) and within that area DBNLs (Part II). Within private law, the study focuses on contractual agreements. More specifically, I will study two specific risk-shifting contracts in Part III, being cyber risk insurance and cyber risk pooling. Section 2.3 will first discuss the general challenges that arise when one aims to utilize legal instruments in cyber security for the purpose of stimulating information diffusion. Hereafter, I will briefly discuss the demarcation of the research by discussing which legal instruments are not included and why. The next section will motivate the selection of legal instruments that are included in the study.

2.3.1 Challenges for the utilization of legal instruments in cyber security

A legal instrument is not a panacea and with its deployment new specific challenges arise.[177] I will discuss two categories of challenges that are important for the positioning the upcoming substantive

[176] The assessment whether regulations are capable of increasing social welfare is one of the core tasks of law and economics (Chang (2000), p. 173).
[177] According to Van Eeten, "cyberlaw provides the most complex and mixed case" (Van Eeten and Mueller (2012), p. 7).

chapters of the study. Within public law, I will discuss the risk of the emergence of governmental failure. Within private law, I will discuss the risk of being subject to the very market failures it aims to solve.

Governmental failure exists when governmental regulation is inefficient.[178] This is the case when the costs of the governmental intervention are higher than its benefits.[179] Within cyber security, the drivers for governmental failure appear ex ante and ex post.[180] Regulation in cyber security is by nature drafted 'top down' by the legislator. These policy makers may have insufficient understanding of the dynamics and incentives on the ground[181] and may be driven by political considerations and agenda setting.[182] The fast changing nature of cyber risk versus relatively slow law-making procedures aggravates the problem. To name an example, it took EU policy makers half a decade to transform the proposal for the European General Data Protection Regulation (hereafter: GDPR) into a regulation. After the adoption of regulation, there is an alarming shortage of good quality ex post impact assessments that measure whether the law actually achieved its societal goal.[183]

With regards to the private law of contracts and torts, the strategic behaviour stemming from market failures such as information deficits, externalities or market power constrains efficiency. For instance, cyber

[178] Coase (1964).
[179] Which is likely to arise in cyber security according to Anderson (2007).
[180] Before and after the adopting legislation.
[181] Van Eeten and Mueller (2012).
[182] Mueller (2004).
[183] Renda (2011); Meuwese (2008).

insurance suffers from moral hazard and adverse selection.[184] Insurers may have incentives to execute a divide and conquer strategy in order to prohibit clients from forming potentially more socially beneficial pooling arrangements. And a final well know issue is the fact that large software players have an incentive to 'dump liability'.[185] The study will take the various types of government and market failure of the legal instruments as such into account, in order to avoid that the medicine will be worse than the disease.

2.3.2 The legal instruments that the study did not include

Within public law, the focus in the study lies on data protection regulation. This regulation is positioned next to numerous other legal instruments not included in the study, for instance legislation related to network and information security (NIS) directive, certification authorities and telecommunications.[186] The effectiveness of those other regulations in aligning incentives in cyber security is often not measured as well. Therefore, future research in this unchartered territory is warmly recommended. The private law of contracts is a so-called 'open system', in the sense that individuals and organizations have the freedom to use its legal concepts. This contractual freedom

---

[184] See Chapter 6; Anderson gives some good examples on why self-regulation of security certificates quickly led to a race to the bottom due to adverse selection issues (2007, p. 14).

[185] Liability dumping is the externalisation of risk to less powerful suppliers or customers, see Anderson, Boehme, Clayton and Moore (2008).

[186] See for instance the NIS Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ; The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) ; At the time of writing the study, EU telecommunication rules were under review, see https://ec.europa.eu/digital-single-market/en/telecoms-rules (accessed on 30 March 2018).

leads to an endless number of possible contracts. But I will solely study two contracts related to risk shifting in Part III. Another large building block from private law is liability. Liability in cyber security is also a promising tool that is potentially capable of internalizing externalities.[187] But, within the study, liability plays second fiddle, in the sense that it will solely be addressed in how it affects data breach notification law and risk shifting.[188]

2.4. A 'Triple Helix' Approach Towards the Specific Issues of the Study

This chapter up until this point further demarcated the study. The focus lies on the role of legal instruments in stimulating information diffusion for the benefit of social welfare. This section will further explain the choice of the specific topics that will be discussed in Part I, II and III. The triple helix approach is introduced as the last building block for the framework of the study along which lines the substantive chapters are placed.

Also, the study up until this point has illustrated the complexity of cyber security. To name a few: the high speed of change of cyber risk, misaligned incentives, inherent insecurity, information deficits, a high risk of regulatory failure and market power of big software and security firms. This leads to the notion of the study that the three main societal actors must work together in the knowledge intensive and complex cyber security theatre. The three societal actors are united in

---

[187] For a general discussion about this capability see Faure (2009).

[188] This does not withstand the fact that liability can play an important role in internalizing social cost (Oded (2012); ENISA (2012)). The literature on liability quite extensive, see for instance Chandler (2006); Crane (2001); August and Tunca (2013); Fryer (2013).

the university-government-industry triple helix.[189] The 'triple helix' was introduced by seminal articles by Etzkowitz and Leydesdorff.[190] The Triple Helix Group of Stanford University describes the field as follows:

> "The concept of the Triple Helix … interprets the shift of a dominating industry-government dyad in the Industrial Society to a growing triadic relationship between university-industry-government in the Knowledge Society. The Triple Helix thesis is that the potential for innovation and economic development in a Knowledge Society lies in a more prominent role for the university and in the hybridisation of elements from university, industry and government to generate new institutional and social formats for the production, transfer and application of knowledge."[191]

The triple helix approach has since been widely used to analyse the tools of the three actors in specific circumstances.[192] The link between

---

[189] "The concept of the Triple Helix of university-industry-government relationships initiated in the 1990s by Etzkowitz (1993) and Etzkowitz and Leydesdorff (1995), encompassing elements of precursor works by Lowe (1982) and Sábato and Mackenzi (1982), interprets the shift from a dominating industry-government dyad in the Industrial Society to a growing triadic relationship between university-industry-government in the Knowledge Society." From Stanford (2017) <https://triplehelix.stanford.edu/3helix_concept> (accessed 30 March 2018). See also Etzkowitz and Leydesdorff (2000).

[190] Etzkowitz (2000); Etzkowitz and Leydesdorff (1995).

[191] Triple Helix Research Group <https://triplehelix.stanford.edu/3helix_concept> (accessed 30 March 2018).

[192] See for instance, Vaivode (2015) in the context of uncertainties; Brem and Radziwon (2017) regarding local niche innovation in Denmark; or the Norwegian innovation system by Strand and Leyesdorff (2013).

the triple helix model and information diffusion has also been pointed out quite clearly:

> "The Triple Helix model assumes that the driving force of economic development in the post-industrial stage is no longer manufacturing, but the production and dissemination of socially organized knowledge."[193]

Also with regards to the cyber security domain, university, government and industry each have their own tools (and handicaps) and can contribute to information diffusion in their own way.

- University has scientific methodology and independence.
- Government has the monopoly on making legislation and violence.
- Industry has the contractual freedom that enables innovation.

In deploying these tools, synergy emerges to the benefit of society. The study will show examples of the tools that universities, governments and industry can deploy in contributing to social welfare in cyber security. A second order effect of the application of the triple helix framework is that the recommendations can lead to increased cooperation and information diffusion between the helices. Scholars in cyber security have already pointed out the roles and responsibilities of the various parties in cyber security,[194] but, to the best of my knowledge, have not thoroughly integrated this in the triple helix framework.

---

[193] Ivanova and Leydesdorff (2014), p. 144.
[194] Van Eeten and Mueller (2013); Kaplan and Rezek (2014).

This study applies or scrutinizes specific tools for the three societal actors. However, it must be noted that on two aggregation levels in this study, the different parties are united.

First, this is an academic study in law and economics. That means that the study inherently learns from the three parties through the lens of the university party and therein the school of law and economics. This notion has consequences for the frame of reference in Part I versus Part II and III. Part I *applies* a tool from university, namely specific university research on DPL. Part II and III *analyses* the effectiveness of tools, already (or potentially) performed by either government or industry. In Part I, I will not scrutinize the tool that I performed myself, for the simple reasons that I am not in the independent position to do that. However, the double-blind peer review process of the published article on which this chapter builds allowed for the desired independent scrutiny.

Secondly, universities, governments and industries are all organizations that are vulnerable for cyber security risk. Consequently, on this level, all three parties belong also to the industry helix. For instance, Part III on the role of industry studies universities as organizations that belong to the industry helix.[195] The relation between the helices is displayed in the figure below:

[195] For instance, Chapter 6 will briefly touch upon the fact that Dutch universities have been subject to an extensive feasibility study concerning cyber risk pooling as a byproduct of this study. In that sense, the universities are just purely a part of Industry.

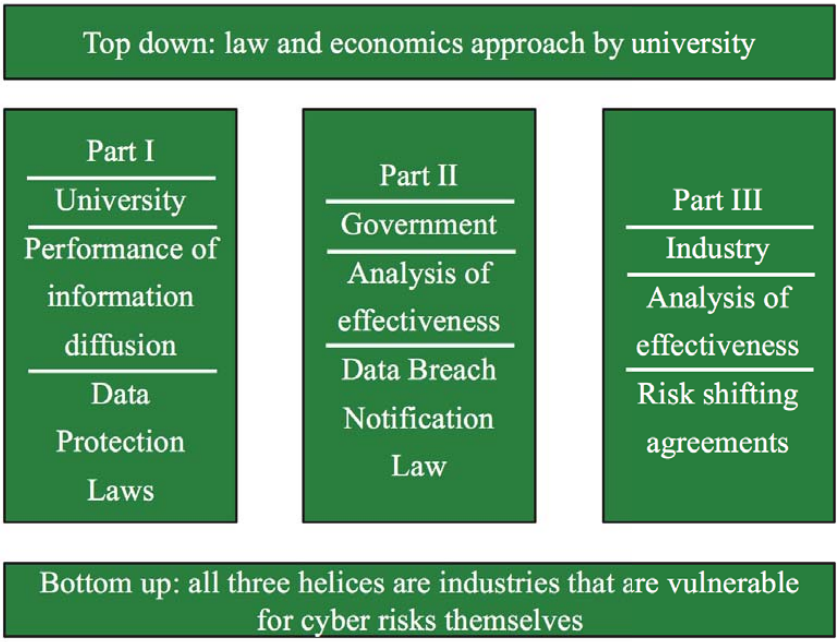


Figure 3: The pillars of the study

The study is structured along the parties of the triple helix.

- Part I will focus on the role of universities and more specific DPLs.
- Part II will focus on the role of governments and more specific data breach notification laws.
- Part III will focus on the role of industry and more specific two risk-shifting contracts, being cyber insurance and cyber risk.

2.5. Information Diffusion and the Triple Helix

This section consecutively introduces the three parts of the study and relates them to the type of information diffusion in the following section.

2.5.1 Part I

Helix. The unique ability of academia is that it can apply scientific methodology in full independence. This has enabled the university helix to produce knowledge since the foundation of the University of Bologna in 1088.[196] The scientific approach of law and economics provides countless possibilities for stimulating knowledge diffusion (in cyber security) and scrutinizing its costs and benefits. I will not include a discussion of roads that law and economics methodology can open, especially because there are comprehensive overviews available.[197] The law and economics approach leads to different types of analyses in this paper regarding the possibilities and effectiveness of the measures the three societal actors can take to stimulate information diffusion. Part I will focus on the application of one methodological approach to one legal instrument to contribute to the overarching law and economics analysis of information diffusion in cyber security. In Part I, the university helix performs the action of diffusion itself, namely by stand alone research. This methodology is called QTA.[198] QTA provides a coded overview of a certain law and its characteristics across countries. By quantifying elements of the law, horizontal comparison between laws is facilitated. This contributes to the diffusion of information. Moreover, the law can be unlocked for statistical analysis by other scholars, for instance in the economics of cyber security. Ergo, QTA directly contributes to ambition 3 of the study, connecting law and economics to the economics of information security. The QTA methodology is applied to DPLs. Data protection is one of the most important and widespread legal instruments in the

---

[196] Some say this is the first *European* University. The research for the study was partly conducted at this university in late 2014 and early 2015.
[197] Parisi (2013); Cooter and Ulen (2004).
[198] I will also not include the discussion whether QTA is officially part of law and economics toolkit or whether it is a method that facilitates empirical research of hypotheses in law and economics.

governance of cyber security. A large number of DPLs has emerged in the past years across the globe but little has been done so far to compare them and thus diffuse and unlock information about these laws. Hence, Part I focuses on the quantification of 71 DPLs using an existing qualitative report provided by DLA-Piper.

Nature of information asymmetry. The question arises which kind of information deficit the QTA analysis aims to solve. Can one say that coding elements of the law creates something 'new', or is it simply an exercise in order to reduce information asymmetry? Can one say that by changing the form of the information, (i.e. from qualitative to quantitative), new information has been created? Before performing the analysis in Part I, the information about the law, more specifically the DPL, primarily was possessed by local lawyers. It was scattered among different legal experts of different countries in different languages. Hereafter, elements in the different qualitative legal texts within 71 countries were structured, translated and grouped by DLA Piper, albeit qualitatively. The analysis in Part I codes this information. I will take the standpoint that a mutation of the information does not alter the very nature of the information, but instead solely fosters the diffusion of information from one place to many others. In that sense, the QTA analysis primarily contributes to the reduction of information asymmetry.[199]

Nature of information diffusion. So now that I have constituted that QTA reduces information asymmetry, the next question is which kind of information is being diffused in this chapter. In a narrow sense, this chapter diffuses information about the DPL. This does not directly lead

[199] One could read the news in the form of a newspaper, on television, in different languages or in the form of statistics. The very nature of the event that occurred does not change.

towards the overarching goal of the study to contribute to social welfare and optimal cyber security investments. In a narrow sense, it merely diffuses information about six characteristics of 71 DPLs. The value of diffusing this information for contributing to the overarching goal of the study – improving social welfare in cyber security – lies in the observation that enhancing information diffusing can reduce transaction costs. It enables a future analysis of the effectiveness of laws, more specifically DPLs, in increasing social welfare. It also enables a ranking of the de jure ability of the law to contribute to privacy control.[200]

2.5.2 Part II

Helix. The government has a monopoly on drafting legislation and using violence by means of a social contract with its citizens, which dictates that the government has a duty of care to protect them.[201] Therefore, the state has special tools that can be deployed to interfere in the cyber security market when it is in the interest of the citizens. In the study, I will not dive further into the normative theories of what does constitute this duty of care and what is the interest of the citizens (this is also to a great extent a political question). I study discuss the specific regulatory tools the government owns in order to execute its duty of care. Instead, it observes the role of government as drafter and enforcer of legislation.

Nature of information asymmetry. Part II will argue that organisations have insufficient incentives to disclose breaches of personal data. This is caused by the experience that, in most situations, the private costs of disclosing data breaches outweigh the private benefits of doing so.

---

[200] I will elaborate on the benefits of information diffusion about DPLs in Chapter 3, Section 3.6.3.

[201] See for instance Rousseau (1762).

Therefore, without a legal instrument in place such as a DBNL, there will be an information asymmetry between the organisation that experienced a data breach on the one hand and the owners of personal data and the public on the other hand.

Nature of information diffusion. I will scrutinize one piece of legislation that potentially can reduce information asymmetry and contribute to the diffusion of cyber security information: the EU DBNL.[202] The concept of the DBNL is that it can force organizations to diffuse information related to data breaches because they have to disclose them to the DPA and/or the general public. To be precise, Part II will study the EU DBNL in the 2018 European GDPR.

2.5.3 Part III

Helix. Industry has the contractual freedom that enables the development of innovative products and services. Some of these innovative products and services stimulate knowledge diffusion. Again, this study will not provide an overview of all innovative products and services on the market. Instead, the industry part of this study will focus on two products that are potentially capable of stimulating information diffusion. It studies two contractual risk shifting agreements.[203] Risk shifting does not provide security directly as typical cyber security products such as network monitoring, virus scanners and firewalls do. Instead, a risk shifting agreement changes incentives at parties.

Nature of information asymmetry. Information regarding the nature of cyber risks (in the form of claim data) and the return on investment of cyber security investments is distributed asymmetrically among

---

[202] As is also recommended by Anderson (2009).
[203] Faure (2009).

actors. Often, actors solely have access to their own loss data and cyber security investment data, which is insufficient to generate a complete picture of the marginal private benefits of cyber security investments. In order to increase social welfare, this data should be diffused and aggregated. Risk shifting methods exactly increase incentives to diffuse and aggregate valuable data regarding the nature of cyber risks and the return on investments of strategies to reduce it.

Nature of information diffusion. When designed properly, risk shifting is capable of increasing incentives for knowledge sharing and diffusion. Within risk shifting, Part III distinguishes risk transfer (insurance) and risk sharing (pooling). Cyber insurance can theoretically result in information diffusion between the insurer and the group of insured. In such a situation, the insurer will collect relevant cyber (claim) data. The information circles back to the insured because the insurer has an interest in providing the insured with accurate information in order to reduce the likelihood of a claim. The developing cyber insurance market with opportunities and challenges will be empirically analysed in the first chapter of Part III. The focus lies at SMEs and the Netherlands.[204] Part III proceeds with Chapter 7 that studies the law and economics of cyber risk pooling, risk sharing without the interference of an insurer.[205] The chapter starts with a discussion of the current theoretical foundations for risk shifting in cyber security. I subsequently discuss cyber risk pooling in relation to individual risk management and cyber insurance. This leads to the formulation of conditions for effective risk pooling in cyber security. The chapter

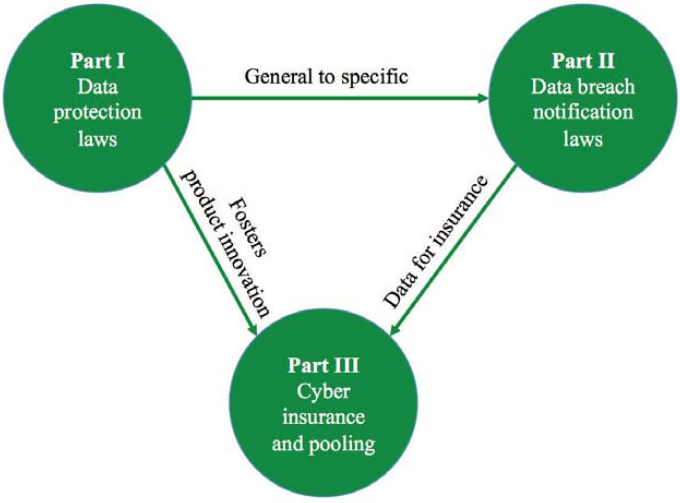
[204] Such as the unavailability of data, uncertainty with regards to insured risks, the prediction of the risk and the absence of an upper bound towards the potential damage (ENISA 2012:10), see for an extensive discussion also Part III
[205] Faure (2009), p.273.

shows that pooling, under some circumstances, may be more effective than cyber insurance.

2.5.4 Connection between the parts

Figure 4 displays the various connections between the three substantive parts of the study. The progression from Part I to Part II entails a transition from general to specific. Whereas Part I focuses on a horizontal comparison of 71 DPLs, Part II will zoom in on one element of the European DPL: the DBNL. Also, Part III has a strong substantive connection with the preceding Parts I and II. In fact, DPLs and data breach notification requirements have driven the development of risk shifting agreements. Stricter DPLs have imposed increased regulatory risk on organizations. Many organizations want to shift this risk. This demand stimulates the development of products and services such as cyber insurance and pooling. DBNLs (especially in the US, where they already were introduced on a state level in 2006) have diffused data breach data that is often indispensable for insurers to calculate their premiums.

Figure 4: Connection between the three substantive parts of the study



Part II and the three chapters of Part III focus on information diffusion *through* legal instruments. The instruments of Chapters 4, 5, 6 and 7 each operate on a different aggregation level. Figure 5 below displays the differences in the scope of diffusion and relevance of the information for individual actors for each instrument:

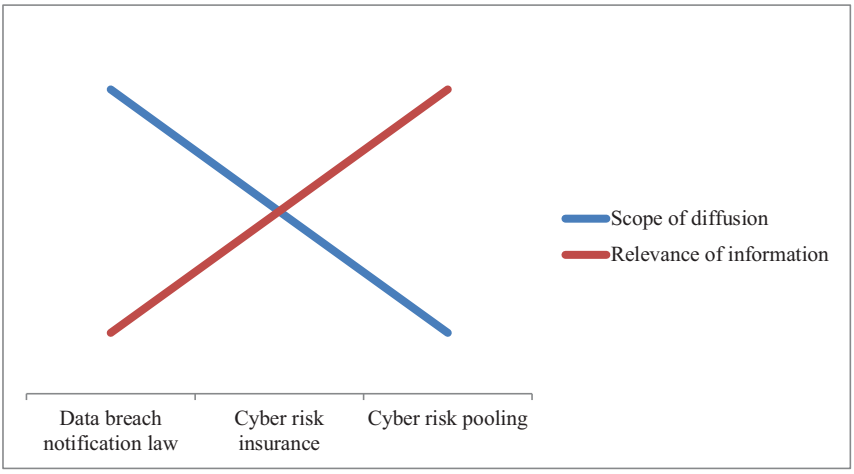


Figure 5: Scope of diffusion versus relevance of information

DBNLs apply to every organization and consequently, the average relevance of the data breach information diffused through the obligation is relatively low. A cyber insurer will need a sufficient number of clients in order for the law of large numbers to function and reduce the risk for the insurer. This will be a subset of the organizations that fall under the DBNL, but still a considerable chunk of society. Also, an insurer can further segment its client base, based on specific characteristics of the clients. The smaller number of participants in a cyber insurance customer base allows for more specific and relevant

diffusion of information.[206] Risk pools are usually much smaller than insurance pools in order to utilize its main comparative advantage: efficient mutual monitoring. This allows insurance pools to diffuse specific and relevant information, but only to a limited number of participants. Hence, in studying cyber insurance and pooling in Part III next to the DBNLs in Part II, and proposing solutions to improve them, the study will contribute to information diffusion on three aggregation levels.

2.6. Summary

Chapter 1 and Chapter 2 have paved the road for the three substantive parts of the study. The overarching structure is displayed in Table 4 below.

Table 4: The structure of the three parts of the study

	Part I	**Part II**	**Part III**	
Helix:	University	Government	Industry	
Legal type:	Public law		Private law	
Specific subject:	71 Data protection laws	EU Data breach notification law	Cyber Insurance market for SMEs	Conditions for cyber risk pooling
Main analysis:	Quantitative text analysis	Analysis of optimal enforcement	Analysis of efficient risk shifting	
Contribution to information diffusion and the reduction of information asymmetry				
Information diffusion	About a legal instrument	Through legal instruments		

[206] Chapter 5 will further elaborate on the differences between cyber insurance and cyber risk pooling.

Nature of information diffusion:	The DPL	Data breaches	Claim data and best practices	Claim data and best practices
Nature of asymmetry:	Qualitative and scattered information	Between organisation and public	Between insurer and insured	Between members of the pool
Other distinctive aspects:				
Empirical Component?	Yes	No	Yes	Yes (but not the main scope)
Year of empirical data/regulation	2014	Entered into force in 2016, applies from 2018.	2015	2017
Geographical scope:	Worldwide	EU	Netherlands	Worldwide / Netherlands
Collaboration Partners:	Economics of Cyber Security Group @ Delft University; Tilburg Institute for Law, Technology and Society, Tilburg University	Dutch data protection authority (Autoriteit Persoonsgegevens)	Economics of Cyber Security group Leiden Delft Erasmus; Eigensteil, Arbinn and Unibarge	Surfnet

Section 2.4 and 2.5 of this chapter discussed the different helices and the specific subjects. Section 2.3 discussed the focus on legal instruments and section 2.1 and 2.2 introduced the focus on information diffusion and the various ways it reduced information deficits. Section 1.2 of the previous chapter discussed the various law

and economics doctrines that are applied throughout the study. The table highlights the prime methodology. Next to the elements that are already discussed, the table list other distinctive aspects of the consecutive chapters. In the first place, the table outlines whether the chapter has an empirical component. Secondly, it displays the year of the empirical analysis (in the case of Chapter 2, the year of the application of the data breach notification legislation). Thirdly, the various geographical scopes of the analyses are displayed. Last, according the procedural strategy, the different cooperation partners per chapter are presented.[207] With chapters 1 and 2, the stage for the cyber security theatre is set. We are now ready to proceed to the first act of the play: quantifying DPLs.

[207] Chapter 1, Section 1.2.3.

PART I:

University

3. QUANTIFYING KEY CHARACTERISTICS OF 71 DATA PROTECTION LAWS

3.1. Introduction[208]

This chapter presents a pioneering analysis that unlocks six characteristics of 71 DPLs.[209] This is, to the best of my knowledge, the first analysis of DPLs in 71 countries.[210] The comparison covers jurisdictions in all continents and 70% of the world population. The analysis benefits the DPL literature by diffusing quantified information about these laws. In this way, the chapter contributes to the studies' overall law and economics notion of the necessity of stimulating information diffusion in order to combat persistent market failures in cyber security. Also, coding discloses these laws for statistical analysis and this benefits the linkage between law and economics and the economics of cyber security. The role of this part regarding the university helix has a fundamentally different point of reference than the other two substantive parts of this study. The analysis in this part is, as such, an action of university that I have performed. This contrasts with Part II and III where the analysis concerns a *scrutiny* of actions of respectively government and industry. In addition, it is important to note that Part I is no more than an example of an academic performance to stimulate information

---

[208] This chapter is based on an earlier publication: Nieuwesteeg (2016). In phases, the text of this chapter can be identical to the text used in this paper. An earlier version of this publication has been listed on SSRN's Top Ten download list for Property Protection.

[209] Except from the naming of the exact name of the DPA, which is not always literally mentioned in the law.

[210] A final limitation of this research is that US DPLs are not considered since these laws are very fragmented over certain sectors and States (Bamberger and Mulligan (2013), pp. 1529-1547); and this chapter aims to, amongst others, contribute to the debate about a federal law by gaining insights on the status of DPLs in other parts of the world. For research on (proposed) US DPLs I refer to Barclay (2013), p. 359.

diffusion in cyber security. There are many other streams of literature contributing to information diffusion in cyber security, which I briefly will address in Section 3.2.2.

Section 3.2 will further introduce the benefits of applying QTA to DPLs. In this section, I will also briefly address the social benefits of the DPL and therein the notion of privacy control, which forms the basis for coding the law. Section 3.3 will discuss the dataset that forms the basis of for coding the law. Section 3.4 will discuss six coded characteristics. Section 3.5 will perform a principal component analysis to distinguish two underlying factors: 'basic characteristics' in the law and 'add-ons'. Subsequently in section 3.6, by combining these two underlying factors, a privacy control index is created. Section 3.7 provides some concluding remarks.

3.2. Quantitative Text Analysis and DPLs

This section will briefly introduce to two main benefits of applying QTA to DPLs. Hereafter; the rationale of DPLs centred in the notion of privacy control will be introduced.

3.2.1 QTA facilitates information diffusion about the law

When one aims to diffuse information about the similarities and differences regarding the widely adopted DPL there are two alternatives: comparative qualitative and QTA. Qualitative legal text analysis is the most common approach among legal scholars. QTA can complement qualitative comparative text analysis.[211] Traditionally, qualitative comparative law entails the analysis, scrutiny and comparison of national legal texts and legal systems.[212] This is done in

[211] Meuwese and Versteeg (2012), p.231.
[212] Zweigert and Kötz, (1998), p.4.

a legal manner: "the comparatists use just the same criteria as any other lawyer"[213], but have "more material at his disposal". For instance, the recent study about DPLs by Bamberger and Mulligan[214] utilizes qualitative comparative legal research focusing on data protection. Through this kind of traditional comparative research, DPLs (and legislation in general) can be understood in detail. However, the qualitative text analysis approach also has drawbacks. A deep dive in a single jurisdiction is time consuming and requires many resources. Consequently, usually a limited amount of jurisdictions can be analysed. Moreover, the results are not suitable for statistical analysis, which has particular relevance for the third ambition of the study in connecting law and economics with the economics of cyber security. QTA, on the other hand, enables a fast overview of laws and facilitates the direct comparison of a limited amount of variables between an extensive number of jurisdictions (in the case of this chapter: 71). In this way, the potential drawback of qualitative legal analysis - its limited number of jurisdictions - can be mitigated. In a globalized world, a quantitative method allows for an enhanced understanding of the similarities and differences between laws.[215] However, nuances within laws and legal systems are omitted in quantitative analysis. Thus, qualitative and quantitative legal analyses can complement each other. Hence, using both yields the best results.

3.2.2 QTA unlocks the law for statistical analysis

Next to its contribution to information diffusion, quantification of DPLs also empowers statistical analysis and in that way, connects law and economics with the economics of cyber security. By quantifying the law, existing theories of effective laws can be falsified or supported,

---

[213] ibid.
[214] Bamberger and Mulligan (2013), p. 1529.
[215] Watt (2006), p. 589.

which creates a better understanding of the law. Additionally, coding is needed to measure effects of laws on events in cyber security. Currently, scholars collect, measure and structure statistics of information security and diffuse information in cyber security. This includes data breaches,[216] deep packet inspection,[217] details of Internet domain names,[218] malware,[219] and e-service adoption.[220] While on the basis of these studies, researchers are able to draw conclusions concerning statistics of information security, this research does not allow for linking effects with differences within regulations. Currently, much legislation is solely described qualitatively. Regulations are displayed in the form of text in a (legal) code, and not as a form of code in an index. For example, a recent study related the intensity of Deep Packet Inspection to strictness of privacy regulation. The researchers encountered difficulties in finding a decent metric for privacy regulation strictness.[221] This exemplifies the demand that researchers in cyber security have for quantitative disclosure of different legislation interfering in the field of cyber security - coded data that is constructed in verifiable way. Measuring the impact of regulations on society improves the quality of the legal system.[222] Coding the law is the first step for such an ex post quantitative impact assessment. In that

---

[216] Nieuwesteeg (2014); Romanosky, Telang and Acquisti (2011)
[217] Asghari, Van Eeten and Mueller (2012a).
[218] Clayton and Mansfeld (WEIS 2014).
[219] Tajalizadehkhoo, Asghari, Gañán et al. (2014).
[220] Riek, Böhme, and Moore (2014).
[221] Asghari, Van Eeten and Mueller (2012b). The index used (the privacy index of Privacy International) was designed in 2007 and is hence out-dated. Moreover, Privacy International does not reveal the methodology of construction. Cybersecurity laws are subject to rapid change. The privacy index gave a value about privacy protection but it was unclear what this value is based upon. Although there were these doubts, Asghari et al. found a significant relation.
[222] Posner (2001)

sense, QTA is a method that facilitates further empirical research in the law and economics of cyber security.[223]

3.2.3 The social benefit of DPLs

The previous section illustrated that QTA applied to DPLs can have multiple benefits, but what is the benefit of DPLs as such? DPLs aim to internalize the benefit of personal data protection at the organization processing this data. Hence, this chapter will solely discuss data protection regarding to natural persons, as Section 1.3.4 also illustrated. Without data protection, the benefits of it for individuals (or the cost of insufficient data protection) are not fully borne by the organization that processes the personal data of the individual. Therefore, there are incentives to underinvest in data protection. These incentives are aggravated by the fact that commercial use of personal information benefits organizations.[224] However, data collection and processing imposes a privacy cost on those individuals that do not want their data being processed for these commercial reasons.[225] This tension has been subject to public debate regarding Facebook privacy settings[226], judicial decisions such as the Google Case (the right to be forgotten)[227] and Google Glass.[228] These events illustrate that organizations may have insufficient incentives to give customers privacy control. In this situation, the market fails in including the costs

---

[223] See for instance the publications in the Journal of Empirical Legal Studies which focusses on the impact of legislation and regulation on society.
[224] Elahi (2009), pp. 113-115; Section 1.3.4.
[225] Akella, Marwaha and Sikes (2014).
[226] See United States of America Federal Trade Commission (2012) <http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf>, (accessed on 30 March 2018).
[227] Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos.
[228] Biometric Technology Today (2013), p. 1.

of those individuals. Hence, DPLs are adopted to correct this market failure and ensure a minimal level of control and protection. DPLs do this by obligating organizations to protect the data of individuals and disclosing data breaches, update individuals about the usage of their data, and allow individuals to alter the user rights of these organizations. DPLs are becoming ubiquitous. By September 2013, 101 countries had implemented a DPL.[229] A few years later, as of May 25, 2018, the GDPR will apply directly in the EU.[230]

3.2.4 The notion of privacy control

The notion of privacy control is closely connected to the social benefit of the DPL. Privacy control forms the core concept from where I will code the law. Hence, this analysis codes those Articles within DPLs that contribute to the notion of 'privacy control'. Privacy control is the notion that individuals should have control over what organizations do with their personal data and the data should be safe and protected by those organizations carrying it.[231] Judges and legal scholars mention the notions of privacy control frequently when discussing the main purpose of DPLs. For instance judge Posner noted that the "economic analysis of the law of privacy … should focus on those aspects of privacy law that are concerned with the control by individuals of the

---

[229] Greenleaf (2014).

[230] Article 99 GDPR.

[231] Personal data is any data that can be linked to individual persons, see Schwartz (1999), pp. 815-817. Some countries need more words than others to describe personal data. See for instance the following examples. Singapore: personal data is data, whether true or not, about an individual who can be identified. South Africa: 'personal Information' includes information relating to both an identifiable, living, natural person, and where applicable, an identifiable juristic person/legal entity. The Netherlands: personal data is any data relating to an identified or identifiable natural person.

dissemination of information about themselves".[232] Privacy control is also the reason why countries adopted DPLs. Control is for instance reflected in European privacy laws. Article 8 of the Charter of Fundamental Rights was the basis on which the European Court of Justice granted individuals control over their data in the Google case.[233]

The effectiveness of privacy control is largely determined by compliance and enforcement. This theory of deterrence assumes that complying with DPLs is to a large extent a cost benefit analysis. Organizations will comply if the cost of compliance is lower than the cost of non-compliance. If a penalty for non-compliance is very high, an organization will be more willing to comply than if a penalty for non-compliance is very low.[234] If enforcement is stringent and hence the likelihood of detection is high, organizations are also more willing to comply.[235] Scholars argue that higher sanctions lead to more compliance.[236] Some argue that employees of an organization are incentivized by the *perceived* severity of the sanctions.[237] Within the context of this chapter, I exclusively look at enforcement mechanisms within the law that increase the likelihood of detection or the height of the penalty.

---

[232] The New Palgrave Dictionary of Economics and the Law (1998), p. 104.
[233] Case (c131-12), par. 99.
[234] Becker (1968), p. 169.
[235] I will more extensively discuss the deterrence theory in Chapter 4, which will also discuss carrots and the expressive function of the law as potential incentive schemes for organizations to comply with the law. It should be noted that the school of behavioural economics disputes the deterrence theory. This school questions its rationality in calculating costs and benefits. However, scholars argue that, when actors tend to be more professional, such as large organizations, their behaviour will be more rational.
[236] Chik (2013), pp. 554-536.
[237] Cheng, Li, Li et al. (2013); DPAs expect fines to be "strongly deterrent", see Grant (2009), pp. 44-49.

Hence, to summarize, the (*de jure*) privacy control perspective in DPLs is interpreted as a combination of the amount of privacy control and the deterrence:

1. The severity of the requirements in DPLs that ensure:
    a. Control: individuals have control over their data.
    b. Safety: personal data is safe in the hands of organizations.
2. The severity of deterrence
    a. Enforcement: mechanisms that increase the likelihood of detection
    b. Sanctions: penalties

Quite naturally, this model for privacy control is not collectively exhaustive. One could think of other variables that influence privacy control such as for instance the 'quality' of the data. Data quality means that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. On the one hand, variables such as data quality can be viewed as a separate indicator for defining privacy control. However, on the other hand, one could also argue that data quality would indirectly influence factor 1a. After all, the above-mentioned four factors were indicated as top level factors for privacy control, but a discussion regarding these factors remains a topic for future research.

Within the literature, there are also objections about the operationalization of privacy as control and protection, for instance the autonomy trap, security seclusion and commodification of privacy.[238]

---

[238] Schwartz (2000): 815 explains the autonomy trap by first assessing this as a problem of self-determination. This is caused by two phenomena. The first is that

Hence, this chapter does not claim a normative standpoint, in the sense that privacy-control should be the best or only aim of DPLs. It takes a neutral descriptive approach. QTA provides a descriptive understanding about those characteristics in the law that contribute to privacy control in DPLs. Moreover, by constructing a privacy control index, it can be falsified or confirmed whether elements of privacy control in the law have an impact on desirable policy outcomes.

3.3. The Dataset

Section 3.3.1 first provides an overview regarding existing datasets that compare DPLs. Section 3.3.2 will substantiate the choice of the DLA Piper dataset, a qualitative overview of DPLs. The texts of these DPL's form the basis of the QTA analysis performed here.

3.3.1 Existing datasets

Comparisons of DPLs that are both academic and quantitative are scarce. Some comparisons are quantitative, but do not reveal their methodology. As a result, their scientific applicability is limited. An example is the index of Privacy International, which uses qualitative descriptions and expert experience to build up an index about the

---

there is a large information asymmetry between the vendor and the consumer, caused by obscure and hard to understand privacy notices (p. 822). The second is the fact that people do not really have a choice to opt out because then they are excluded for services. Information asymmetry and little choice causes a general inertia toward default terms. Moreover, autonomy is limited further through the legitimate use of personal data by the government or other parties. The use of personal data by third parties also causes the security seclusion problem: people think they have control and information is isolated, but this is not the case. The last problem consists of the commodification of privacy, it can be traded and sold at the lowest price. More about this in the work of Schwartz.

degree of privacy protection in a country.[239] However, the way in which this index is constructed is unclear. Moreover, other indices, such as 'heat maps' made by law firms, are based on the expert judgement of legal experts.[240] Those heat maps indicate that European and other developed countries have the most stringent DPLs in the sense of privacy control, although in the latest rankings there are some newcomers such as Mauritius.[241] The definition of privacy control varies, and the method of construction of the indexes is sometimes not entirely clear. Moreover, studies contradict each other. For instance, DLA Piper regards Iceland as having limited protection and enforcement while the Webindex places Iceland in its top 10. The scores of these indices are shown in Appendix B.

Table 5: Quantitative studies on DPLs

Firm	**Definition of privacy control**	**Percentage of top 10 that is an EU country**	**Percentage of top 10 that is an developed country[242]**
Heatmap DLA piper 2012-2014	Degree of enforcement and protection measures of data protection. (Note: the actual study is qualitative in	75%	100%

[239] See Privacy International (2007) <http://observatoriodeseguranca.org/files/phrcomp_sort.pdf> (accessed 30 March 2018).
[240] Interview Mr. Richard van Schaik (July 23, 2014).
[241] Appendix B displays the values of all the parameters of the data protection heat maps.
[242] Upper quartile in the human development index 2014.

	nature, solely the additional 'heatmap' is a quantitative score based on expert judgement)		
Webindex 2014	To what extent is there a robust legal or regulatory framework for protection of personal data in your country?	64%[243]	86%
Privacy International 2007	Degree of privacy enforcement (subset of the index)	71%	100%

Other comparisons are merely qualitative. This stream of literature describes the origins of the laws and their embedment in legal cultures. There is much qualitative comparative legal research on DPLs. Hence, this overview only highlights a few examples. Current qualitative studies state that European laws have the most advanced data protection regimes.[244] Greenleaf for instance argues that non-western DPLs are influenced by the EU,[245] implying the EU sets the standard. In qualitative research, privacy control is naturally interpreted as a broader concept than the data protection legislation as such. For instance, Bamberger and Mulligan indicate that the dynamics between public and private actors are possibly of more importance than formal

[243] The Webindex included relatively more non-western countries.
[244] Boillat and Kjaerum (2014), p. 3.
[245] Greenleaf (2012).

legislation.[246] A DPL should be nested within broader ethical frameworks to function correctly.[247] Hence, there is a difference between 'law in the books' and 'law in practice'. It is on the basis of these insights important to note that this chapter solely takes into account 'law in the books'.[248]

Another problem is time. Information technology is dynamic, and so are the laws governing it. Hence, information security laws, such as DPLs, are increasingly subject to change. Governments are becoming progressively more concerned with online privacy. As a result, studies regarding Internet related legislation become quickly out-dated. 20 out of the 71 laws I analysed were introduced or had significant amendments in 2012, 2013 or 2014. One study of the United Nations is scientific, quantitative and recent, but focuses on a different subject: cybercrime legislation.[249] According to one of the co-authors, one of the key challenges of quantifying laws is making meaningful categorizations while keeping variety in variables low in order to avoid over- interpretation.[250] In Table 6, I scored current studies and their limitations regarding application in this study.

[246] Bamberger and Mulligan (2013), pp. 1529-1648.
[247] ibid.
[248] ibid.
[249] UNODC (2013).
[250] Interview Ms. Tatiana Tropina (June 2, 2014).

Table 6: Comparative studies and their limitations

Study	Limitations			
	Methodology not revealed	Not quantitative	Out dated or limited	Different subject
National privacy ranking [251]	V		V	
The Webindex (Subparameter: personal data protection framework) [252]	V			
Internet privacy law: a comparison between the United States and the EU [253]		V	V	
A comparative study of online privacy regulations in the US and China [254]		V	V	
UNODC Comprehensive study on cybercrime ([255]				V
The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108 [256]		Partial[257]		
Privacy in Europe, Initial Data on Government Choices and Corporate Practices [258]		V	V	

[251] Privacy International (2007)
[252] World Wide Web Foundation (2012) <https://webfoundation.org/research/the-2012-web-index> (accessed on 30 March 2018).
[253] Baumer, Earp and Poindexter (2004), p. 400.
[254] Wu, Lau, Atkin et al. (2011), p. 603.
[255] UNODC (2013).
[256] Greenleaf (2012).
[257] The Greenleaf study quantifies several characteristics of non-European DPLs. The aspects are quantified on a dummy scale but no final index is constructed.
[258] Bamberger and Mulligan (2013), p. 1529.

Data protection 1998-2008 [259]		V	V	
New challenges to data protection [260]		V		
European privacy and human rights 2010 [261]		V	V	

3.3.2 The dataset adopted: the DLA Piper data protection handbook

As discussed, the analysis capitalizes on the text of the DPLs as the main source for coding the law. An assessment of legal texts requires knowledge regarding the origins of the laws and local legal language. How do we gather the knowledge we need with limited resources? The answer lies in the fact that local legal experts are able to efficiently extract characteristics of the law from the literal text. Global international law firms have such local experts. Therefore, I relied on reports on data protection legislation constructed by international law firms to serve their clients. There are several reports available as displayed in Table 7 below:

Table 7: Summary of current qualitative data protection law comparisons

Name	Firm	Last updates	Coverage (number of countries)
Global Data Protection Handbook [262]	DLA Piper	2013-2014	71
International Compendium of Data Privacy Laws [263]	Baker Law	2014	42
Data Privacy Heat Map	Forrester	2014	54 (only available for paying clients)

[259] Grant (2009), p. 44.
[260] Korff and Brown (2010).
[261] Privacy International (2010).
[262] DLA Piper (2014).
[263] Baker Law (2014).

I use the DLA Piper Global Data Protection Handbook as the main source due to two reasons. First, it is the most complete report, covering 71 laws. Second, the validity of the data is assured; the information is the direct representation of the law and not the interpretation of experts according to a DLA Piper partner that I interviewed.[264] The authors of the DLA piper report do not discuss any *de facto* aspects of the law. Different experts of partners or offices of DLA piper delivered the information. With regards to the other reports, I could not reach the authors of the International Compendium of Data Privacy Laws by Baker law. The Forrester report is only available for paying clients and thus not usable.[265] I will not use the previously discussed quantitative 'heatmap' of DLA-Piper, which is based on expert judgement. Instead, I will solely use the qualitative texts in the DLA Piper Data Protection Handbook.

3.4. The Six Coded Characteristics

This section discusses the coded six characteristics. The characteristics that have been coded were selected in four steps.

1. The characteristics need to affect one or more of the four predefined aspects of privacy control.
2. The characteristics need to be quantifiable. The characteristics are coded on a relatively 'rough' dummy or interval/ratio scale in order to avoid over-interpretation.[266]

---

[264] I extensively interviewed one of the authors. Interview with one of the main experts (core team) of the report, Richard van Schaik (July 23, 2014); naturally, the QTA analysis is quantitative, but the criteria are still scored by human experts.
[265] I asked for disclosure for academic purposes but did not get a response from the firm.
[266] Interview Tatiana Tropina (June 2, 2014).

3. The characteristics need to be different among countries. If all countries would have the same variable, this variable will not elicit differences between countries.
4. For simplicity, I allowed for a maximum of six characteristics.

Table 8 provides an overview of the effects of characteristics on various elements of privacy control. The footnotes highlight choices made in the coding process.[267] Excluded characteristics can be found in the long list in Appendix A.[268]

Table 8: Characteristics and their contribution to privacy control

Aspects of privacy control (horizontal)	**1. Requirements**		**2. Deterrence**	
Characteristics in the law (vertical)	**1a. Control**	**1b. Safety**	**2a. Enforcement**	**2b. Sanctions**
Data collection requirements	1			
Data breach notification requirement	1	1		
Data protection officer		1	1	
Data protection authority			1	

[267] There are more relevant characteristics that are worth researching. This should be one of the key next steps for future research. For instance, requirements for processing and security guidelines are for example arguably also a proxy for privacy control. But processing requirements are roughly equal over all countries. A quantification of those requirements would not elicit differences between DPLs. Security guidelines are hard to quantify on a dummy or interval scale.
[268] This chapter omits other characteristics of DPLs, for instance the general requirement for fair and lawful processing of personal data.

Monetary Sanctions				1
Criminal Sanctions				1
Characteristics per determinant	2	2	2	2

In the next sections, I will discuss each individual characteristic.

3.4.1 Data collection requirements

Data collection requirements prescribe that organizations should interact with data owners before personal data collection.[269] Hence, data collection requirements affect the amount of control that individuals have over their personal information.[270] There are roughly two forms: an information duty and prior consent. An information duty means that individuals have to be informed about data collection and processing.[271] Prior consent means that individuals have to give consent before a data processor wants to disclose personal information.[272] An information duty is less severe, since organizations are not dependent on the consent of consumers and consumers might miss this information.[273] In Table 9 below, the results for collection requirements are shown.

---

[269] Collecting data is often distinguished from processing personal data. Collection requirements can differ from processing requirements. Processing requirements are mostly stricter. Most states that have an information duty for collecting data require prior consent for processing data. Hence, this would not leave much space for differences between laws, and therefore the focus of this chapter lies in collecting data.

[270] Whitley (2009), p. 154.

[271] The exact form varies. Some states require a purpose of use on the website (Japan). Other require 'making reasonable steps to make the individual aware' (Australia).

[272] Le Métayer and Monteleone (2009), pp. 136-137.

[273] Data collection requirements also have their disadvantages. Typically, consumers have to give consent for long pages of privacy rules and organizations

Table 9: Descriptive statistics data collection requirements

Characteristic	Function	State	Code	Results
Requirements for collecting personal data	Requirements (Control individuals)	Prior consent needed	2	55
		Information duty only	1	10
		No requirement / no law	0	6

The data shows that most countries require prior consent. Only a few require an information duty. This is not surprising, since prior consent is one of the corner stone principles of many DPLs. Countries that are labelled zero (no requirement) also do not have a DPL at all.

3.4.2 Data breach notification law

The data breach notification requirement (in the US this is commonly referred to as the data breach notification law (DBNL) influences both control and safety requirements in privacy control. A notification requirement obliges organizations to notify a data breach to affected customers and a supervisory authority. Schwartz and Janger suggest that this is a constructive measure because the quick awareness of a data breach by consumers has a positive impact on control of data of

---

do not have the obligation to check whether consumers understand these obligations. Hence, there are some new initiatives to enhance the communication about privacy, for instance the Dutch 'datawijzer', see Nationale Denktank (2014) <http://nationale-denktank.nl/jaarlijkse-denktank/datawijzer/> (accessed on 30 March 2018, Dutch).

individuals.[274] A notification of a data breach also ensures safety of data. The damage following a breach can be mitigated faster.[275] Moreover, a requirement incentivizes organizations to invest in information security.[276] Organizations want to avoid a notification because of the perceived reputational damage and administrative cost they suffer. The descriptive statistics for data breach notification requirements across the 71 states analysed are displayed below in Table 10.

Table 10: Descriptive statistics data breach notification requirements

Characteristic	Function	State	Code	Results
The existence of a Data Breach Notification Law	Requirements (Safety of data) (Control – mitigation measures)	DBNL	1	21
		No DBNL	0	50

21 out of 71 countries that were studied have a DBNL.[277] This possibly has to do with some concerns regarding administrative burdens for organizations. However, in 2018, the GDPR applies in the EU and consequently, all Member States (hereafter: MS) will have a DBNL, increasing the number of DBNLs by 18 countries to 39 countries. This contrasts with the situation in the United States, which was not included in the analysis. The State of California already adopted a

[274] Schwartz and Janger (2007), p. 971.
[275] The following Chapter 4 will address this more thoroughly.
[276] Romanosky, Telang and Acquisti (2011), p. 256
[277] This low amount of DBNLs contrasts with the US (which is not a part of this study). California was the first state to adopt a DBNL in 2003 and other states quickly followed. As of 2014, 46 out of 50 US States adopted a DBNL.

DBNL in 2003. Since this point in time, these laws have been widespread in the US - 47 out of its 50 states have a DBNL.

3.4.3 Data protection authority (DPA)

A DPA has to enforce the DPL.[278] The presence of a DPA is an indicator of the degree of compliance and indicates that there are resources for enforcement. A DPA executes security audits and imposes sanctions. DPAs review organizations based on complaints of individuals.[279] The actual degree of enforcement and modus operandi differs between countries[280], and is excluded from this analysis. Apart from enforcement, DPAs are an information and notification centre. For instance, organizations should notify a data breach to the DPA according to a DBNL. Moreover, the importance of privacy and data protection can be visible for consumers when a DPA is adopted. For instance, DPAs communicate through media channels to educate individuals about who to complain to for (alleged) breaches of data protection.[281] Thirdly, a DPA functions as a point of contact, which eases and urges compliance with DPLs. Without a DPA, enforcement would merely be passive in the sense that probably only non-compliance highlighted in the media would be sanctioned. The descriptive statistics of the presence of data protection authorities are displayed in Table 11 below.

---

[278] Wong (2011), p. 53.
[279] Bamberger and Mulligan (2013), pp. 1529-1613.
[280] See for instance Schütz (2012) <http://regulation.upf.edu/exeter-12-papers/Paper%20265%20-%20Schuetz%202012%20-%20Comparing%20formal%20independence%20of%20data%20protection%20authorities%20in%20selected%20EU%20Member%20States.pdf>, a comparison of four DPAs in a case study format (accessed 30 March 2018).
[281] Wong (2011), pp. 53-56.

Table 11: Descriptive statistics of the presence of data protection authorities

Characteristic	Function	State	Code	Results
The presence of designated data protection authorities (DPAs) to enforce the law	Compliance	DPA present[282]	1	58
		No DPA	0	13

The analysis shows that most countries (58) have a DPA. This can be explained by the central place that DPAs have in the implementation of DPLs. 13 countries have no DPA. Most countries that do not have legislation also do not have a DPA - except Saudi Arabia and Thailand, who have a DPA but no legislation yet. This research did not account for differences between various DPAs.[283]

3.4.4 Data protection officer (DPO)

A data protection officer (hereafter: DPO) is responsible for safeguarding personal data of individuals. A DPO ought to be appointed by organizations to ensure compliance.[284] Hence, a DPO captures both elements of 'safety' and 'compliance'. A DPO functions as a connection between the text of the law and the daily practice of organizations that process personal data. Organizations with DPOs are

[282] A DPA is coded 1 if there is a DPA is required and in place. In the case of the Philippines, a DPA is named in the law, but is not constituted yet. Therefore, it is labeled '0'.

[283] For instance, the severity and intensity of enforcement, but also the degree of independence of a DPA with respect to the government. Several parameters of DPAs can be used as a proxy of the intensity of enforcement, for instance the annual budget of the DPA, the height and frequency of imposed penalties and the ability and frequency of executed security audits.

[284] Kayworth, Brocato and Whitten (2005), pp. 110-115.

more likely to incorporate a privacy policy. DPOs aid to establish social norms within this corporate infrastructure.[285] Privacy minded employees induce compliance in the whole organization because of social norms.[286] The descriptive statistics of the presence of a DPA are displayed in Table 12 below:

Table 12: Descriptive statistics of the presence of data protection officers

Characteristic	Function	State	Code	Results
Every organization has to assign a DPO to ensure compliance	Compliance	DPO[287]	1	17
		No DPO	0	54

17 DPLs require a DPO; this is less than a quarter of the total amount of laws observed. The requirement to appoint a DPO could be an administrative burden for organizations, which could explain why most countries did not incorporate this requirement.[288]

3.4.5 Monetary sanctions

Monetary sanctions aim to increase the cost of non-compliance. Interviewees suggested that managers in organizations are deterred by

[285] Cheng et al. (2013) p. 447; Kayworth, Brocato and Whitten (2005), p. 110.
[286] Bamberger and Mulligan (2013), pp. 1529-1611.
[287] Laws that have a general obligation for organizations to appoint DPOs are labelled 1. Some laws only require a DPO for designated sectors. This is not a general obligation; hence they are labelled '0'. Other laws reduce data breach notification requirements if a DPO is appointed. Since this is not an obligation to install a DPO, these states are labelled '0'. The same applies with laws that recommend organizations to install a DPO.
[288] ibid.

the maximum damage possibly incurred by non-compliance.[289] Hence, the characteristic 'monetary sanction' relates to the maximum sanction that can be imposed. The descriptive statistics of the height of monetary sanctions are shown in Table 13 below:

Table 13: Descriptive statistics of the height of monetary sanctions

Characteristic	Function	State	Code	Results
The maximum penalty for non-compliance with the regulation	Compliance	Above 1M[290]	1	5
		Between 100k and 1M	.75	18
		Between 10k and 100k	.5	25
		Under 10k	.25	13
		No penalty at all	0	10

Only 5 out of 71 countries have a maximum penalty for non-compliance above 1 million euro. When taking into account that the likelihood of detection is low, it can be argued that de facto deterrence starts from sanctioning levels above 1 million euro.[291] Hence most DPLs have a limited deterrent effect. The likelihood of being caught is

[289] For instance as indicated in an interview with Mr. Richard van Schaik.
[290] Furthermore, sanctions that are displayed in other currencies are converted into euros. Average USD EUR currency = 1.35, Australian 1.4, Canadian 1.45, GBP 0.83. Also, sanctions are grouped in order of magnitude. The sanctions are not corrected for purchasing power.
[291] See Chapter 4 for an extensive discussion on the deterrent effect.

likely to play a large role in determining the expected sanction. This likelihood is strongly related to the enforcement costs for DPAs, which are high according to scholars, but unobserved in this analysis.[292]

3.4.6 Criminal sanctions

The possibility to impose criminal penalties for non-compliance with the regulation can be considered as an additional sanction. Personal accountability increases when persons are subject to criminal sanctions such as imprisonment. Hence, criminal sanctions cause personal responsibility for the actions of corporate employees. The descriptive statistics of the criminalization of non-compliance with DPLs is shown in Table 14 below. Approximately half of the countries I studied criminalize non-compliance with the DPA.

Table 14: Descriptive statistics of criminal penalties

Characteristic	Function	State	Code	Result
Criminalization of non-compliance with the regulation	Compliance	Criminalization[293]	1	38
		No Criminalization	0	33

3.4.7 Correlations between the individual characteristics

Table 15 below shows the internal relation of the characteristics as such. EU membership and developed countries are also included. Solely significant correlations are displayed.

---

[292] Grant (2009), pp. 44-49.

[293] Solely provisions that specifically criminalize non-compliance with the DPL are labelled '1'. General criminalization clauses are excluded, because every country criminalizes intentionally causing harm.

Table 15: Pearson correlation between individual coded characteristics **, Correlation is significant at the 0.01 level (2-tailed)

Correlations									
		EU_member	Penalty_crim	DBNL	DPO	DPA	Req_Collect	Penalty_eur	Upper quartile HDI
EU_member	Pearson Correlation					.365**	.369**		.456**
	Sig. (2-tailed)					.002	.002		.000
Penalty_crim	Pearson Correlation								
	Sig. (2-tailed)								
DBNL	Pearson Correlation								
	Sig. (2-tailed)								
DPO	Pearson Correlation								
	Sig. (2-tailed)								
DPA	Pearson Correlation						.324**	.384**	.341**
	Sig. (2-tailed)						.006	.001	.004
Req_Collect	Pearson Correlation							.378**	
	Sig. (2-tailed)							.001	
Penalty_eur	Pearson Correlation								
	Sig. (2-tailed)								
Upper quartile HDI	Pearson Correlation								
	Sig. (2-tailed)								

EU membership is correlated with the presence of a DPA, strong requirements for data collection, and the upper quartile of the Human Development Index. This makes sense since the European Directive 95/46/EC requires the presence of a DPA and prior consent before collection.[294] Moreover, almost all EU MS are in the upper quartile of the Human Development index. Furthermore, it is notable that DPA presence is correlated with collection requirements and monetary

[294] This is also required by the GDPR.

sanctions. This also makes sense: a legislator that constitutes a DPA is likely to give this guarding dog some extra teeth in the form of high monetary sanctions.

3.5. Identifying Underlying Unobserved Variables

3.5.1 Principal component analysis

A principal component analysis is a decent tool to determine whether the six characteristics can be explained by fewer underlying factors. The advantage of the principal component analysis is that it can reduce noise in the coded characteristics, by identifying an underlying variable. Hence, by performing this analysis, the results gain in stability, because the effect of randomness in the coded characteristics is reduced. In theory, the data is suited for principal component analysis, with a significant Kaiser-Meyer-Olkin Measure of Sampling Adequacy above .6 (.671) and a significant Bartlett's test for sphericity (p=0.003).

3.5.2 Basic and advanced characteristics

Two factors have eigenvalues above one.[295] Moreover, the scree plot - the diagram displaying the eigenvalues, shown in Appendix A.5 - displays a relatively clear bend between the second and the third suggested factor. The pattern matrix shows clear correlations of each characteristic with one particular underlying factor. The correlation with the individual characteristics are shown in Table 16 below.

Table 16: Correlation of individual characteristics with their underlying factor * = .05 significance level, ** = .01 significance level

Factor 1: basic characteristics	Factor 2: advanced characteristics

[295] The widely used direct oblimin rotation with kaiser normalisation is applied.

Presence of data protection authority (.766**)	Data protection officer (.729**)
Requirements of collection (.720**)	Data Breach Notification Requirement (.669**)
Monetary penalties (.745**)	Criminal penalties (.461**)

The first factor is called 'basic characteristics'. The distribution of the scores for this factor are displayed in the figure below.

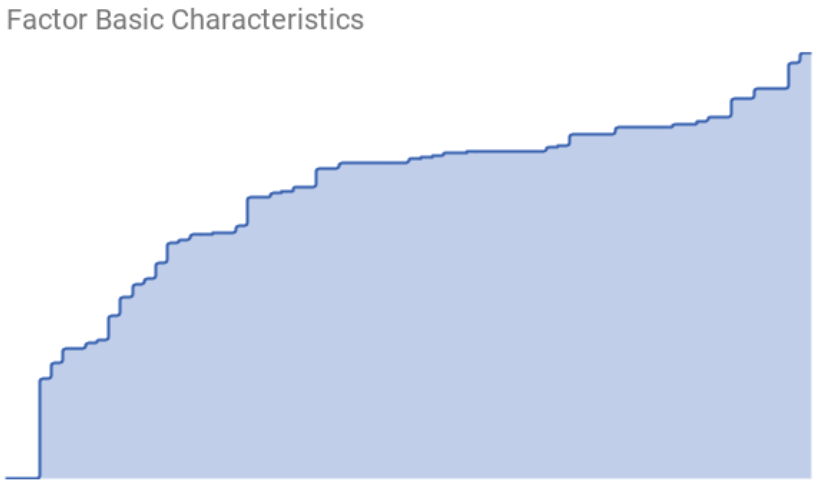


Figure 6: Distribution of scores for factor 'basic characteristics'

What stands out is that the distribution is quite flat, which means that a large part of the countries have similar scores for this factor. Only at the beginning of the graph (low scoring countries) and at the very end (very high scoring countries) much difference is observed.

Furthermore, the factor has positive and significant correlations with:

- the Webindex '13 (.532**) and '14 (.584**),
- the Privacy index '07 (.373*),

- the DLA piper heatmap score (.495**)
- and EU membership (.415**).

Hence, the three underlying characteristics are basic building blocks of many DPLs.

The second factor is called 'advanced characteristics'. The distribution of the scores for this factor are displayed in the figure below.

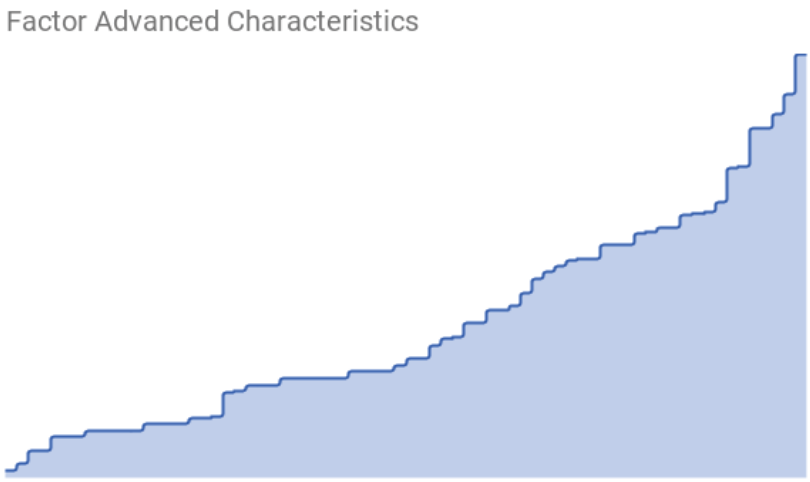


Figure 7: Distribution of scores for factor 'advanced characteristics'

Relative to the factor 'basic characteristics', the distribution of 'advanced characteristics' is much steeper, indicating that there is a large difference between the countries with regards to the three underlying characteristics in the DPLs.
Moreover, they are only positively correlated with laws that have been amended recently (.301*),[296] which might indicate that these characteristics were added later.

[296] After excluding countries without a DPL.

3.6. Aggregating Underlying Factors towards a 'Privacy Control Index'

3.6.1 The privacy control index

The privacy control index is the sum of the two factors, 'basic characteristics' and 'advanced characteristics'. Hence, the index does not resemble the top 10 of 'best' DPLs. However, it resembles those DPLs that scored high on the presence of the six underlying characteristics (see Table 17).

Table 17: Top ten countries of the privacy control index

Rank	**Privacy control index**
1	Mexico
2	South Korea
3	Taiwan
4	Philippines
5	Germany
6	Mauritius
7	Italy
8	Luxembourg
9	Norway
10	Israel
# Developed countries | # EU countries	7/10 | 2/10

Based on the literature, I would expect high positions for developed and European countries. However, non-western and underdeveloped countries such as Mexico, Mauritius, Taiwan and the Philippines occupy a significant part of the top 10. On the other hand, the bottom 10 countries also mainly consist of non-developed and non-EU countries, which partly have no DPL at all. Countries such as Mexico

and Taiwan recently adopted DPLs.[297] These countries have laws with high *de jure* standards. This might indicate that legislators may want to keep up with developed countries. Recent international calls for stringent privacy regimes could explain this. Now that the GDPR applies, all 27 MS will occupy the top position again based on the privacy control index. EU countries now have a middle- position in the index. The presence of those countries in the bottom 10 of the index is due to the fact that these countries have very limited or no DPLs.

The overall distribution of the index, composed of the sum of the factors 'basic characteristics' and 'advanced characteristics' is displayed below.

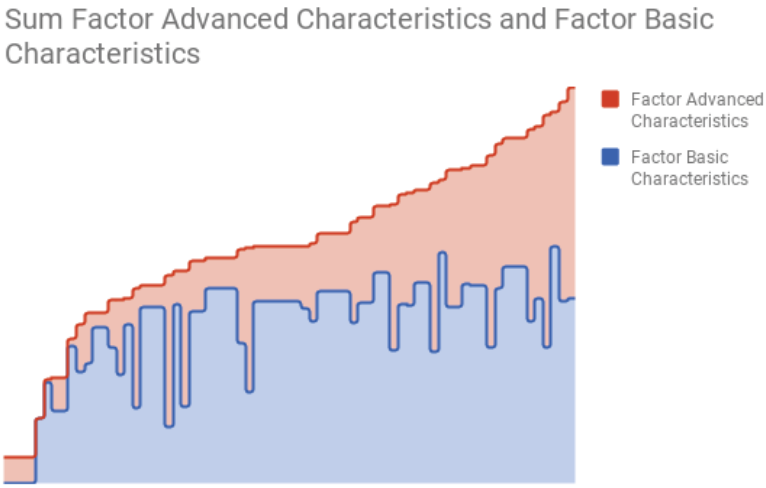


Figure 8: Privacy index as the sum of two factors

Overall, one can distinguish a double s-shaped curve with roughly three phases. First, on the left side of the chart, low scoring countries

[297] The introduction date of non-western countries: Mexico (2011), South Korea (2011), Mauritius (2009), Taiwan (2012), South Africa (2013), Philippines (2012).

can be observed which still have to implement the most 'basic characteristics'. Second, in the middle of the chart, countries can be observed that in general implemented 'basic characteristics' but still lack most advanced characteristics. And third, at the right side of the graph, one can observe that the factor 'advanced characteristics' largely determines the top position of a country in the index. Surprisingly, there is a steep increase at the right side of the chart, which could indicate rapid legal development at the top.

3.6.2 Relation with other indices

Table 18 shows correlations of the privacy control index with other indices that were discussed.

Table 18: Correlation with known indices **significant on the 0.01 level; *significant on the 0.05 level

Correlation statistics	Cases (countries)	Index
Heat map DLA piper	64	.353**
Webindex 2014	49	.542**
Webindex 2013	49	.475**
Privacy International[298]	42	Not significant

The privacy control index does correlate with the heat map of DLA (based on a one digit score expert judgment of the authors). The privacy control index does not correlate with the privacy index of Privacy International. This can be explained by the fact that this index is seven years old, while 20 out of 71 laws have been amended since. There are significant correlations with the two versions of the

[298] As far as the index of Privacy International is concerned, both the total index as well as the subindex for statutory protection is used. Both indices did not have a significant correlation with the privacy control index.

Webindex. There is no significant correlation between the date of adoption of the law and the last date of amendment.[299] The low correlation with other indices could support the argument that the analysis has added value, because the question arises to which extent expert judgments differ from the substantiated QTA analysis.

3.6.3 Explanatory power of the index and the coded characteristics

The preceding sections described the process of coding six characteristics of DPLs. The six characteristics that were selected express an estimation of privacy control in the DPL.[300] Hereafter, these six characteristics were grouped in two factors. The sum of these factors resembles the privacy index. This section will discuss the benefits of the privacy index and the underlying characteristics.

In essence, the discussion regarding the benefits and validity of the analysis in this chapter reaches the heart of the 'de jure – de facto' debate in empirical legal studies. Some scholars argue that the law as such, without taking into account implementation, execution or enforcement, cannot solely give an indication on its impact on society. In other words: the 'de jure' text does not provide a reliable predication regarding 'de facto' impact. For instance, during the process of writing this chapter, a discussant provided the example of the constitution of the Democratic People's Republic of Korea (DPRK). From a purely de jure point of view, this constitution would gain a high position on an

---

[299] For this analysis, states without a DPL are excluded, because otherwise there would be always a very high correlation between the data of adoption or amendment and the privacy control index.

[300] The privacy index displays not perfect representation of *de jure* privacy control. For instance, a limited amount of characteristics is used through a secondary source on dichotomous or ordinal scale.

imaginary 'constitution index'.[301] However, it goes without saying that the constitution of the DPRK is merely or hardly a façade for a regime that is known for the most severe violations of almost every aspect of that same constitution. This example illustrates the carefulness one should have when coding, structuring and analysing legal texts. It stresses the importance of avoiding any qualification of the quantified output without any further analysis. This argument especially holds when the analysis is performed on an aggregated level (i.e. the index level of the privacy index). On such an aggregated level, it is impossible to analyse and disentangle the effects of individual characteristics.

However, the fact that a claim of the significance of an index cannot be made straightforwardly does not mean that it is impossible to extract valuable information from a modelled or simplified version of the law. The value of QTA strongly depends on the interpretation and utilization of the data. One could recall the famous quote of the British statistician George Box, which said: "all models are wrong, but some are useful".[302] Analogous to the example of the DPRK, the privacy index does not straightforwardly provide a ranking of the quality of real privacy control in the countries that have been subject to this analysis. Instead, a further synthesis has to be performed in order to extract its value. Accordingly, I will provide some arguments of the usefulness and benefits of the analysis and index below.

1. High positions do not necessarily implicate high standards, but low positions could implicate low standards with regards to privacy control.

---

[301] Such a constitution index would code the protection that the constitution gives to the rights and freedoms of citizens.
[302] Box and Draper (1987), p. 424.

Analogues to the example regarding the constitution of the DPRK, one cannot state that the high position of countries such as Mexico or Mauritius should result in the conclusion that citizens have a high degree of privacy control in these countries. Still, one could argue that an adequate legal data protection structure is a first condition for attaining desired privacy control outcomes. In other words: having a legal framework for privacy control is the starting point for building privacy control in a democratic society. This could indicate that countries with low positions in the index have low de facto standards with regards to privacy control. Countries with high positions at least made 'a first step'. The benefit of the quantification procedure lies in the fact that a quantified index is better capable of quickly diffusing information about the absolute ranking of countries relative to a qualitative document such as the DLA-Piper report that describes each country individually. The index will for instance be useful for policymakers and scientists in order to study below average performing countries in order to move them in a more desirable direction with regards to de jure privacy control.[303]

2. When breaking down the index into its underlying factors or on a characteristics level, there is a possibility to demonstrate or falsify the effectiveness of the individual elements of the law by relating them to other dependent variables.

The discussion above, which focusses on the relation between the law and its impact, is theoretical in nature. The considerations purely remain (substantiated) hypotheses. The benefit of the privacy control index, and especially when it is broken down into the underlying

[303] One should take into account exceptions to this argument such as the ranking of common law systems.

characteristics, lies in its ability to actually measure the impact of these laws. For instance, one could relate each individual characteristic to several proxies for privacy control and analyse in which way de jure privacy control influences de facto privacy control. When performing such an analysis, it is very important to control for other variables that might influence the effectiveness of the law or set up a measurement method eliminates or reduces the influence of the environment.[304] In other words, the analysis is the starting point for falsifying or confirming various hypotheses about the impact of laws within the 'de jure de facto' debate.

3. QTA is necessary for deriving historical legal trends and the adoption and evolution of de jure standards.

When performing QTA on DPLs regularly, for instance annually, an indication can be made of the absolute and relative positions of countries in the index. This allows for analyses over time on the adoption of several characteristics of the law. For instance, one could analyse the pace at which the DBNL will spread among other

[304] For example, the de facto (actual) enforcement of DPLs by the authorities, the number of security audits, their capacity and budget, Internet usage per capita, the number of virus scanners installed and the number of data breaches per year affect privacy control. It is an option to incorporate some of these factors in future versions of the privacy control index. Some of them cannot even be observed directly and it is certainly impossible to incorporate all of them. They can only be measured through the usage of proxies, such as the intensity of metrics that are measurable, such as the amount of deep packet inspection, or surveys among citizens; Greenleaf (2014), p. 10. As an example: I also did not consider the sociological and political background of the countries that have adopted DPLs; for instance, governmental access to medical, financial and movement data, data retention and transborder issues. Privacy International analyses and groups these aspects of privacy per country. See <www.privacyinternational.org> (accessed 30 March 2018).

countries. This for instance can contribute to the theory of legal transplantation.[305] This index made a first step to open this kind of analysis for other researchers.

3.6.4 Limitations

There is an inherent limitation to the explanatory power and the benefits of the analysis performed in the chapter. This is related to the fact that the coding process has been performed in the form of a secondary analysis; by using a qualitative report provided by DLA-Piper. In an interview with one of the authors of the report, it became clear that the legal experts solely collected the data from the various legal text, often written in local legal language.[306] Hence, I assume that the text in the report is transparent in the sense that it is solely the summary of text of local DPLs. Still, a risk remains that errors are made by these experts.

However, one should be aware that errors can also be made by academic researchers. There are quite strong incentives for DLA-Piper to reflect accurate information: this commercial report aims to inform clients, often multinationals, and is made by one of the largest law firms in the world. Verification of the report by analysing the local laws directly is relatively straightforward but time consuming. In order to further mitigate this issue, I only used variables that are hardly vulnerable for misinterpretation by experts, for instance the height of the sanction for not complying with the law (see Section 3.4). Overall, I recognize that the use of the DLA-piper report indeed slightly reduces the clarity of the analysis. However, in my opinion, the quality of the report in combination with the enormous decrease in time consumption of the analysis makes this trade-off acceptable.

---

[305] Watson (1974).
[306] See Section 3.3.2.

3.7. Concluding Remarks

This chapter coded the following six characteristics based on the text of 71 DPLs: data collection requirements; the data breach notification requirement; the presence of a DPA; the requirement of a DPO; the level of monetary sanctions; and the presence of criminal sanctions. QTA facilitates information diffusion about the law and the connection of law and economics with the economics of cyber security.

The results show that 5 out of 71 countries have a maximum penalty for non-compliance above 1 million dollars. 55 out of 71 countries require prior consent before collecting personal data and 10 have an information duty. 21 out of 71 countries have an obligation to notify data breaches, while in the US, 47 out of 50 states have such a DBNL. Most of the countries observed - 54 out of 71 - do not require a DPO. About half the DPLs analysed have criminalized non-compliance with the DPL. Principal component analysis is used to distinguish two underlying factors called 'basic characteristics' and 'advanced characteristics'. The final privacy control index is constructed by combining these factors. EU MS have DPLs with privacy control above average but no absolute top position but this will change in 2018 when the GDPR will apply. Moreover, countries that are not known for their stringent privacy control such as Mauritius and Mexico occupy a top position in this index. Countries that have low privacy control in DPLs are always non-European and mostly outside the upper quartile of the Human Development Index.

Although this overview of DPLs undoubtedly is a snapshot, it will likely keep its relevance. The analysis allowed for empirical analysis with metrics dating from the timeframe of construction. Also, it provided an accessible overview of DPLs, which supports scholars that aim to map the (historical development of) different aspects of Internet governance and regulation. Future research could update this privacy

control index and incorporate more characteristics and countries that have a DPL. For instance, the GDPR replaces all DPLs on Member State level on May 25 2018 and will have a major impact on the position of these countries in the index. Future updates allow recognizing patterns in the development of DPLs over time. One might also code the literal text of the law, instead of depending on (validated) sources of international law firms such as DLA Piper. A more ambitious contribution would be to add de facto indicators such as strictness of enforcement of the law, for instance by using proxies such as the amount of penalties imposed by data protection authorities.

With regards to the ambitions of the study, the overview in this chapter provides a further linkage between law and economics and the economics of cyber security. From now on, scholars in the economics of cyber security can perform econometric analyses that relate concepts in DPL to certain security metrics such as for instance deep packet inspection. These future analyses can eventually empirically verify whether concepts within DPL, for instance data breach notification requirements, contribute to the stimulation of information diffusion. The next chapter will further discuss one data breach notification requirement in depth. More specifically this chapter will provide a law and economics analysis of the upcoming EU DBNL.

Appendix A

Appendix A.1. The six characteristics

Table 19: The Six Characteristics

Country	Last_ amendment	Req_Collect	DBNL	DPA	DPO	Penalty_ eur	Penalty_ crim
Argentina	2000	2	0	1	0	1	1
Australia	2014	1	0	1	0	4	0
Austria	2000	2	1	1	0	2	0
Belgium	2001	2	0	1	0	3	1
Brazil	No DPL	0	0	0	0	0	0
British Virgin Islands	No DPL	0	0	0	0	0	0
Bulgaria	2013	2	0	1	0	2	1
Canada	2000	2	0	1	1	2	0
Cayman Islands	No DPL	0	0	0	0	0	0
Chile	2009	2	0	0	1	1	0
China (People's Republic)	No DPL	2	0	0	0	2	0
Colombia	2013	2	1	1	0	3	0
Costa Rica (2013)	2013	2	1	1	0	2	1
Cyprus	2003	2	0	1	1	2	1
Czech Republic	2000	2	0	1	0	3	0
Denmark	2000	2	0	1	0	2	1
Egypt	No DPL	2	0	0	0	0	0
Finland	2000	2	0	1	0	2	1
France	2004	2	0	1	0	3	0
Germany	2009	2	1	1	1	3	0
Gibraltar	2006	2	0	1	0	1	1
Greece	2012	2	0	1	0	2	1
Guernsey	2001	2	0	1	0	2	0
Honduras	2006	2	0	1	0	0	0
Hong Kong	2013	1	0	1	0	3	1
Hungary	2012	2	0	1	0	2	0
Iceland	2000	2	0	1	0	2	1
India	2013	2	0	0	1	3	1
Indonesia	2008	2	1	0	0	2	1
Ireland	2003	2	1	1	0	3	0
Israel	2006	2	0	1	1	3	1
Italy	2003	2	1	1	0	3	1

Japan	2005	1	1	0	0	1	1
Jersey	2005	2	0	1	0	4	1
Lithuania	2003	2	1	1	0	1	0
Luxembourg	2006	2	1	1	0	3	1
Macau	2005	2	0	1	0	2	1
Malaysia	2013	2	0	1	0	2	1
Malta	2003	2	1	1	0	2	1
Mauritius	2009	2	1	1	1	1	1
Mexico	2011	1	1	1	1	4	1
Monaco	2008	2	0	1	0	2	1
Morocco	2009	0	0	1	0	2	1
Netherlands	2001	2	0	1	0	1	0
New Zealand	1993	1	1	1	1	0	0
Norway	2000	2	1	1	0	3	1
Pakistan	No DPL	0	0	0	0	0	0
Panama	2012	1	0	1	0	3	0
Peru	2013	2	0	1	0	3	1
Philippines	2012	2	1	1	1	3	1
Poland	2007	2	0	1	1	2	1
Portugal	1998	2	0	1	0	2	1
Romania	2001	2	0	1	0	2	0
Russia	2006	2	0	1	1	1	0
Saudi Arabia	No DPL	0	0	1	0	0	0
Serbia	2012	2	0	0	0	1	1
Singapore	2014	2	0	1	1	4	0
Slovak Republic	2013	2	0	1	1	3	0
South Africa	2013	1	1	1	1	2	1
South Korea	2011	2	1	1	1	2	1
Spain	1999	2	0	1	0	3	0
Sweden	1998	2	0	1	0	2	1
Switzerland	1992	2	0	1	0	1	0
Taiwan	2012	2	1	1	0	4	1
Thailand	No DPL	1	0	1	0	0	0
Trinidad and Tobago	2012	2	0	0	0	0	0
Turkey	2012	1	0	1	0	1	1
Ukraine	2014	1	0	0	1	1	1
United Arab Emirates	2007	2	1	1	0	1	1
United Kingdom	2000	2	0	1	0	3	0
Uruguay	2009	2	1	1	0	2	0

Appendix A.2. The full privacy control index and the two underlying factors

Table 20: The full privacy control index and the two underlying factors

Country	Sum_Factors	FAC_basic_characteristics	FAC_add_ons
Mexico	2,80	0,50778	2,29023
South Korea	2,55	0,45472	2,09537
Taiwan	2,38	1,42940	0,95054
Philippines	2,33	-0,34448	2,67775
Germany	2,11	0,51623	1,59089
Mauritius	2,07	0,10804	1,96393
Italy	1,90	1,08273	0,81910
Luxembourg	1,90	1,08273	0,81910
Norway	1,90	1,08273	0,81910
Israel	1,82	0,70158	1,11743
South Africa	1,60	-0,35891	1,96163
Costa Rica	1,42	0,73605	0,68766
Malta	1,42	0,73605	0,68766
Singapore	1,38	0,76309	0,61295
Cyprus	1,34	0,35490	0,98599
Poland	1,34	0,35490	0,98599
Jersey	1,17	1,32958	-0,15884
India	1,12	-0,44430	1,56837
Colombia	0,98	0,79756	0,18318
Ireland	0,98	0,79756	0,18318
United Arab Emirates	0,95	0,38937	0,55622
Slovak Republic	0,90	0,41641	0,48151
Indonesia	0,73	-0,40983	1,13860
Belgium	0,69	0,98291	-0,29028
Peru	0,69	0,98291	-0,29028
Austria	0,50	0,45089	0,05174
Uruguay	0,50	0,45089	0,05174
Canada	0,42	0,06974	0,35007
Bulgaria	0,21	0,63623	-0,42172
Greece	0,21	0,63623	-0,42172
Monaco	0,21	0,63623	-0,42172
Portugal	0,21	0,63623	-0,42172
Lithuania	0,02	0,10421	-0,07970
Hong Kong	-0,02	0,34261	-0,35830
Denmark	-0,02	0,46289	-0,48744
Finland	-0,02	0,46289	-0,48744
Iceland	-0,02	0,46289	-0,48744

Macau	-0,02	0,46289	-0,48744
Malaysia	-0,02	0,46289	-0,48744
Sweden	-0,02	0,46289	-0,48744
New Zealand	-0,04	-1,16409	1,12855
Russia	-0,06	-0,27694	0,21863
Czech Republic	-0,23	0,69774	-0,92620
France	-0,23	0,69774	-0,92620
Spain	-0,23	0,69774	-0,92620
United Kingdom	-0,23	0,69774	-0,92620
Gibraltar	-0,26	0,28955	-0,55316
Argentina	-0,26	0,28955	-0,55316
Japan	-0,46	-1,39680	0,93913
Australia	-0,46	0,40413	-0,86278
Ukraine	-0,54	-1,77795	1,23746
Guernsey	-0,71	0,35107	-1,05764
Hungary	-0,71	0,35107	-1,05764
Romania	-0,71	0,35107	-1,05764
Chile	-0,75	-1,42282	0,66957
Panama	-0,94	0,05745	-0,99422
Serbia	-0,96	-0,85633	-0,10222
Turkey	-0,97	-0,35074	-0,62118
Netherlands	-1,18	0,00439	-1,18908
Switzerland	-1,18	0,00439	-1,18908
Morocco	-1,20	-0,64435	-0,55777
China (People's Republic)	-1,40	-0,79482	-0,60670
Honduras	-1,66	-0,34229	-1,32052
Egypt	-2,36	-1,48817	-0,86958
Trinidad and Tobago	-2,36	-1,48817	-0,86958
Thailand	-2,37	-0,98258	-1,38854
Saudi Arabia	-3,08	-1,62287	-1,45657
British Virgin Islands	-3,77	-2,76875	-1,00563
Cayman Islands	-3,77	-2,76875	-1,00563
Brazil	-3,77	-2,76875	-1,00563
Pakistan	-3,77	-2,76875	-1,00563

Appendix A.3. Long list of characteristics

This appendix displays all the characteristics in the long list.[307] I also give a description why the characteristics are excluded. An explanation of the included characteristics can be found in the main text. The criteria for exclusion are as follows:

1. Allowance for a maximum of six characteristics to avoid too much complexity.
2. The six characteristics are in total a proxy for the four aspects privacy control in the letter of the law: control, safety, enforcement and sanctions.
3. The proxies need to be quantifiable, in the sense that they can be coded on a dummy or interval/ratio scale.
4. The characteristics are different among countries

Table 21: Long list of characteristics

Characteristics	**Why excluded?**
Data collection requirements: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	Included
Data quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	It is assumed that this characteristics less a characteristic for control than the data collection requirement and the breach requirement. Therefore the latter two are prioritized.
Purpose specification: The purposes for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to	Not meeting criterion 4. A use limitation is present in all DPLs.

[307] Greenleaf (2012); OECD (2013); Council of Europe (1981); DLA Piper (2014).

the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	
Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with its purpose except: a) with the consent of the data subject; or b) by the authority of law	Not meeting criterion 4. A use limitation is present in all DPLs. (this is the core of the existence of DPLs)
Security safeguards: Personal data should be protected by reasonable security safeguards against such risk as loss or unauthorised access, destruction, use, modification or disclosure of data.	I assume that security safeguards are important but ancillary to the more high level DBNL and privacy officer. For instance, the latter can implement the security safeguards.
Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller	Not meeting criterion 3. The concept of openness is hard to quantify.
Individual access: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial	Similar to the argument related to security safeguards, individual access is relevant insofar an individual actually knows that his data is used. Hence individual access is ancillary to the data control requirement.
Individual correction: to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.	Similar to individual access.
Accountability: A data controller should be accountable for complying with measures which give effect to the principles of the DPL.	Not meeting criterion 4. In all DPLs, data controllers are accountable.
Requirement of an independent **data protection authority** as the key element of an enforcement regime	Included

Requirement of **recourse to the courts** to enforce data privacy rights	Not meeting criterion 4. In all DPLs, one has a recourse to courts. (apart from the countries that do not have a data protection law at all)
Requirement of **restrictions on personal data exports** to countries which did not have a sufficient standard of privacy protection (defined as 'adequate')	Ancillary to the data collection requirement.
Collection must be the **minimum necessary** for the purpose of collection, not simply 'limited'	Ancillary to the data collection requirement.
A general requirement of '**fair and lawful processing**' (not just collection) where a law outside Europe adopts the terminology of 'fair processing' and a structure based on other obligations being instances of fair processing, this is both indicative of influence by the Directive, and makes it easier for the law to be interpreted in a way which is consistent with the Directive;	Not meeting criterion 3. The concept of 'fair and lawful processing' is hard to quantify.
Requirements to notify, and sometimes provide '**prior checking'**, of particular types of processing systems	Ancillary to and extension of the data collection requirement
Destruction or **anonymisation** of personal data after a period	Ancillary to and extension of the data collection requirement
Additional protections for particular categories of **sensitive data**	Ancillary to the data collection requirement and the security safeguard requirement.
Limits on automated decision-making, and a right to know the logic of automated data processing	Ancillary to and extension of the data collection requirement.
Requirement to provide '**opt-out**' of direct marketing uses of personal data	Ancillary to and extension of the data collection requirement
Monetary sanctions for non-compliance with the DPL	Included
Criminal sanctions for non-compliance with the DPL	Included
The requirement to install a **DPO**	Included
A **Data Breach Notification Law** requirement	Included

Appendix A.4. Overview of coded characteristics

Characteristic	State	Code
Requirements for collecting personal data	Prior consent needed	1
	Information duty only	.5
	No requirement / no law	0
The existence of a DBNL	DBNL	1
	No DBNL	0
The constitution of designated data protection authorities (DPAs) to enforce the law	DPA required and constituted	1
	No DPA	0
Every organization has to assign a data protection officer (DPO) to ensure compliance	DPO required	1
	No DPO	0
The maximum penalty for non-compliance with the regulation	Above 1M	1
	Between 100k and 1M	.75
	Between 10k and 100k	.5
	Under 10k	.25
	No penalty at all	0
Criminalization of non-compliance with the regulation	Criminalization	1
	No Criminalization	0

Appendix A.5. Scree Plot Principal Component Analysis

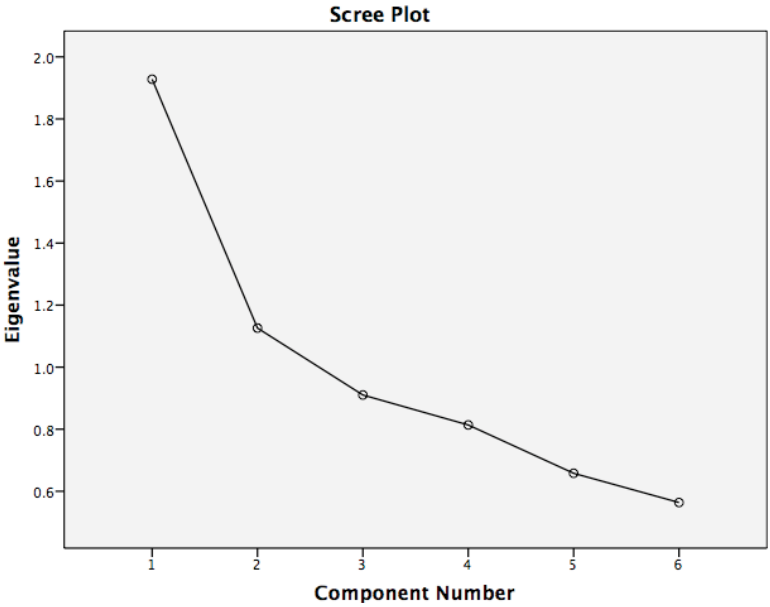


Figure 9: Scree plot of principal component analysis

PART II:

Government

4. DATA BREACH NOTIFICATION LAWS: CARROTS, STICKS AND THRESHOLDS

4.1. Introduction[308]

This chapter will perform a law and economics analysis on the European Union DBNL (Hereafter EU DBNL or the DBNL) as incorporated in Articles 33 and 34 of the GDPR. The EU DBNL imposes an obligation on organizations to disclose certain breaches of personal data to a notification authority and to affected individuals. I will analyse the following question: whether and under which conditions will the current design of the EU DBNL be effective in increasing social welfare? I will propose recommendations for the ex post execution and enforcement of this important piece of legislation.[309] The de jure text of the DBNL is definite and will not change in the near future.[310] However, many of the design choices can be implemented during the ex post execution and enforcement of the law. Therefore, the upcoming

---

[308] This chapter is based on a working paper by Nieuwesteeg and Faure (2018) presented at the 34th annual conference of the European Association of Law and Economics (EALE), the 13th annual conference of the Italian Association of Law and Economics (SIDE) and the 17th Annual Workshop on the Economics of Information Security (WEIS). In phases, the text of this chapter can be identical to the text used in this working paper. In the pursuit of this joint working paper, I made an independent and definable contribution. However, views and errors remain my sole responsibility.

[309] Those breaches of personal data can be both analogue and digital. In practice, the loss of personal data is mostly cyber related, because the majority of personal data records is stored online in our digitalized society. In this chapter I will primarily focus on personal data breaches in the digital society.

[310] After all, there have been more than two decades in between the entry into force of Regulation 2016/679, and its predecessor, Directive 95/46/EC.

social welfare analysis also has value for policy makers in the field after the entry into force of the law.[311]

My core methodology will be a law and economics analysis of incentives and optimal enforcement.[312] In addition, I will utilize the stream of literature on the effectiveness of DBNLs in the US. In the US, most states have a DBNL and consequently there is empirical data regarding the data breach notifications.[313] This stream of literature has covered regulatory impact,[314] effectiveness in reducing identity theft,[315] economic effects,[316] perceptions from the private sector[317] and the need to integrate the state level laws into a federal law.[318] But, the differences between the two legal regimes are large with respect to data breach notification regulation. To name a few examples: In the US, on the one hand, class actions are a much more significant cost for organizations. However, on the other hand, in the US administrative penalties of DBNLs are usually two orders of magnitude lower than in the EU DBNL. In the EU, data protection in general is much more strictly regulated, especially in the GDPR. Also, in the EU the DBNL is

---

[311] The study builds upon the social welfare literature, which is one of the corner stones of micro-economic analysis. See amongst many others: Cooter and Ulen (2016); Arrow (1963); Bergson (1938); Varian (2010), p. 634.
[312] For instance Polinsky and Shavell (2005).
[313] In 2017, 48 out of 50 states in the US have adopted a DBNL. See NCSL (2017) <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> (accessed 30 March 2018) for the actual status. Only Alabama and South Dakota did not have a DBNL at the time of writing this chapter.
[314] Winn (2009), p. 1133.
[315] Romanosky, Telang and Acquisti (2011), pp. 256-262.
[316] Lenard and Rubin (2009), Boehme (2012) uses a theoretical model and also involves EU law.
[317] Mulligan (2007).
[318] Bisogni (2015).

regulated on a central level instead of at the state level in the US. Hence, I will take the peculiarities of the EU legal regime into account in order to facilitate the transplantation of the lessons learned on the other side of the Atlantic.

To the best of my knowledge, a law and economics analysis of DBNLs in the EU has not been performed yet.[319] A thorough (ex ante and ex post) scrutiny of the effects of the DBNL is interesting for the EU and for the effectuation of its data protection policy.[320]

This chapter is structured as follows. Section 4.2 introduces the EU DBNL, its origins, aims and its embedment in the extensive legislative data protection package labelled as the General Data Protection Regulation 2016/679. In section 4.3, I discuss the social costs and benefits of the DBNL relative to the threshold of notification. Section 4.4 discusses whether organizations have sufficient incentives to notify, in the absence of the law. I discuss the reasons to believe that these incentives are likely to be insufficient and come to the conclusion that a market failure is likely to exist in the absence of regulation. Section 4.5 discusses whether and in which cases the DBNL is justified in correcting this market failure. In doing so, I also take the public costs of the regulation into account. Section 4.6 continues the discussion by analysing whether the current legislative design of the upcoming DBNL is capable of inducing organizations to notify at acceptable social cost. The section discusses several socially ideal design choices

---

[319] Such an analysis did not take place on a Member State level. Some EU countries, such as Germany, Ireland, Italy, Lithuania, Luxemburg, Malta and the Netherlands independently adopted a DBNL before the entry into force of the GDPR. See also Chapter 3, Section 3.4.2.

[320] The only research I am aware of scrutinizing the EU DBNL is from De Hert and Papakonstantinou, who take a more legal approach (De Hert and Papakonstantinou (2016), pp. 179-194).

for optimizing the social potential of the DBNL and compares them with the actual choices made by the EU legislator. I will also discuss incentive schemes related to the implementation of the DBNL that the EU legislator did not include in the literal text of the DBNL, such as the enforcement of sticks, the use of carrots and the expressive function of the law. Section 4.7 discusses the optimal notification threshold and section 4.8 will provide some concluding remarks.

4.2. The European Union Data Breach Notification Regulation

This section will briefly introduce the origins and specific characteristics of the EU DBNL. The DBNL is part of the GDPR. The GDPR regulates many aspects related to the processing of personal data such as basic principles (Article 5), lawfulness of processing and individual consent (Article 6) and rights of individuals that have provided their data to a third party (section 2 of the GDPR). The GDPR has entered into force on May 24 2016 and shall apply after a two year transition period in May 25 2018.[321] Contrary to its predecessor, Directive 95/46/EC, the GDPR will equally apply directly to every citizen and organization falling within the scope EU law.[322] Hence, the GDPR will be an influential piece of legislation. The GDPR arranges the DBNL in Articles 4(12), 33, 34 and 83(4):

Article 4 (12) defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' The definition thus focuses on the consequences of the data breach. In doing so, the EU legislator

[321] Article 99 GDPR.

[322] Directive 95/46/EC (the 'Data Protection Directive') did not contain a requirement to notify data breaches.[322]

incorporates the 'CIA triad' of confidentiality, integrity or availability of personal data.[323] Possible differences in the origin of the data breach, for instance whether a data breach is intentional or negligent, do not matter.

Articles 4 (7) states which entities have to notify data breaches. These 'data controllers' can be legal persons or public authorities. Hence, the DBNL applies to both public and private organizations.

Article 2 (2) excludes certain data breaches from the notification duty. Data that (a) falls outside the scope of EU law; (b) falls within the scope of Chapter 2 of Title V of the TEU; (c) is carried out by a natural person for personal use or (most notably) (d) is used for the execution of criminal prosecution do not have to be notified when breached.

Articles 33 and 34 regulate the actual obligation to disclose a data breach.[324] There is an apparent difference in notifying a data breach to a DPA (Article 33) or to the individual affected (Article 34). With respect to the former, an organization has to notify the DPA 'unless the personal data breach is 'unlikely' to result in a risk to the rights and freedoms of natural persons'.[325] Hence, this 'likelihood' is the key threshold for notifying the DPA. Article 33 (1) further specifies that the notification should be as soon as possible, and not later than 72 hours after the data breach. However, this is apparently not a red line, because if it is unfeasible to do so, the organization can notify later, but

---

[323] Pfleeger (2003), p. 504;

[324] The obligation applies to every organization, with some minor exceptions listed in Article 2 GDPR.

[325] As such, it is quite peculiar that the Article speaks of a likelihood *to result in* a risk, since risk also contains the element of likelihood. (risk = likelihood * impact), see Chapter 1, Section 1.3.1. Hence, within this chapter, I will just use the term risk.

has to specify the reasons why it does so. Under 33(3), the organization has to include the nature of the breach, its consequences for individuals, a description of countermeasures undertaken and a contact point. When possible, the organization should also include the type and number of affected individuals and the number of records being breached.

Article 34 shows that the threshold for mandatory notification to individuals is higher on several points compared to notifying the DPA ex Article 33. First and foremost, notification to consumers is only mandatory when the data breach is 'likely to result in a 'high' risk to the rights and freedoms' of individuals. Hence, where in Article 33 a certain risk suffices, in the case of Article 34 the risk should be 'high'. The GDPR does not specify this gap between risk and high risk any further.[326] With regards to the temporality of notification, Article 34(1) solely determines that this should be without undue delay and does not specify the 72 hours of Article 33. Also, the organization does not have to describe the nature of the data breach and the number of individuals affected when notifying to individuals. Article 34(3) heightens the threshold even further. This article provides three possible arguments that organizations can use not to communicate to individuals. First, organizations may refrain from notifying individuals when the data is made sufficiently difficult to use, for instance through the use of encryption. Secondly, when the organization has taken 'subsequent measures' which ensures that the high risk will no longer materialize they do not need to notify. Thirdly, notification to individuals is not necessary when it would put a disproportionate burden on the organization. Ergo, there is quite a large difference in the execution of notification to the DPA and the individual. Quite surprisingly, the GDPR does not state the reasons for

[326] De Hert and Papakonstantinou (2016), pp. 179-194

this difference to exist. However, Article 34(4) regulates that the DPA may require from the organization to still issue an additional notification to individuals when the DPA assesses that the likelihood of adverse consequences for individuals is 'high' according to Article 34(1).

Article 83(4) states that a sanctions of €10,000,000 or 2% of the undertakings turnover, whichever is higher can be imposed when an organization fails to notify a data breach.[327] These sanctions are high when compared sanctions in the US, whereby state level DBNLs usually have sanctions in the magnitude of $100,000s or lower.[328]

4.3. The Social Benefits and Costs of the DBNL

This section discusses the social benefits and costs of the DBNL generally.[329] The starting point here is that the social benefits of the DBNL depend on the disclosure threshold. Section 4.3.1 will further introduce this 'threshold perspective'. Section 4.3.2 will discuss the social benefits of a DBNL, while section 4.3.3 will discuss its social costs.

4.3.1 The threshold

The EU legislator defines the data breach notification threshold. The GDPR defines this as data breaches that result in a 'risk to the rights and freedoms of natural persons' in the case of notifying to the DPA

---

[327] Article 83 (4) GDPR; Article 83 (2) GDPR specifies guidelines for the determination of the actual height of the sanction.
[328] Nieuwesteeg (2014).
[329] Law and economics literature labels an activity as 'socially optimal' if the additional social ('marginal') costs of the activity equal marginal benefits thereof. See, among many others, Shavell (2004); Cooter and Ulen (2016); Schäfer and Ott (2005);
Faure (2009), see also the discussion in Chapter 1, Section 1.4.

(Article 33). In the case of notification to affected individuals this risk should be 'high' (Article 34).[330] Naturally, some data breaches are more risky than others.[331] Identity theft has a high risk, credit card theft has lower risk and the theft of certain passwords and usernames of non-vital websites as well as encrypted data have almost no impact on the lives of individuals.[332] Hence, theoretically, these data breaches can be plotted on a risk continuum. The two thresholds within the EU DBNL are certain points on this risk continuum, which can currently not exactly be determined because of the ambiguous threshold definition by the EU legislator (see Section 4.2). This chapter discusses to what extent the social outcomes of the law change when the risk threshold is interpreted more or less strictly and consequently more or less data breaches have to be notified. To be precise, I will observe the drivers for a change in private and social optima when the threshold shifts.[333] Section 7 will also discuss whether it is socially desirable to distinguish between thresholds for notifying to the DPA and to the individuals affected. In the upcoming sections, I will primarily focus on the private and social benefits and costs of notification to individuals ex Article 34 GDPR. Section 7.1 will address the different position that the notification obligation to the DPA has.

---

[330] See Section 4.2.

[331] This chapter does not aim to provide an extensive overview of personal data breaches and their risk for individuals, organizations and society. For the potential consequences of personal data breaches and their risks for individuals and organizations see inter alia Verizon (2017).

[332] Article 33 (3) GDPR under c ; Compare for instance the steam hack which also included credit card theft, but also less vital username information (Johnston (2011) <https://arstechnica.com/gaming/2011/11/valve-confirms-steam-hack-credit-cards-personal-info-may-be-stolen/> (accessed 30 March 2018).

[333] I assume that along X-axis of notification significance, a breach concerns a similar amount of records (being affected consumers).

4.3.2 The social benefits

This section will discuss the social benefits of data breach disclosure to individuals. First, and for the GDPR foremost, the social benefit of data breach disclosure is the effectuation of the individuals' 'right to know' that their data is compromised. This 'right to know' is an aspect of the fundamental right on the protection of personal data, enshrined in the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights.[334] The protection of personal data has been the primary reason for the EU to adopt the GDPR and therein the EU DBNL.[335] The social benefit of the 'right to know' is quite intangible. Also, its intrinsic value varies among schools of thought. On one side of the spectrum, there is a stream of literature that prioritizes fundamental rights by qualifying it as 'a first line of defence'.[336] On the other side of the spectrum, there is literature that argues that the right to know has little value[337], supported by empirical research that evaluates the low monetary value consumers attach to this right.[338] In a democratic society, the valuation of the right to know will be decided by the policy-maker according to the preferences of the voter. But the value of the right to know will strongly depend upon the nature of the data breach. For example it may be more important for an individual to be aware of an identity theft than of the loss of a

---

[334] Article 8 of the Charter of Fundamental Rights of the European Union) and Article 8 of the European Convention of Human Rights. The right to know is described clearly in Article 8(2) of the Charter, which states that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"

[335] Article 1 GDPR.

[336] Arnbak (2016).

[337] Posner (1998).

[338] Cofone (2015).

username or password for a Steam account (a platform for mobile gaming).[339]

Secondly, data breach disclosure will result in additional incentives for data security improvements at individuals and organizations. The literature has labelled this effect 'sunlight as disinfectant'.[340] There are short and long term effects and direct and indirect effects of data breach disclosure. Data breach disclosure has a short term direct impact on mitigating and avoiding consumer[341] and organizational losses.[342] However, organizations and individuals may overinvest in their security improvements.[343] On the long term, data breach disclosure can foster "cooperation between information security departments", according to US chief security officers.[344] This diffusion of information has positive effects on overall security.[345] Also, indirectly, a data breach disclosure raises the general public's awareness regarding cyber security. Similar to the right to know, I assume that the 'sunlight as disinfectant' benefit for security improvement is lower when the significance of the data breach risk is lower.

---

[339] This gradual decrease occurs independently of the absolute value of the right to know, which as said has to be determined by societal debate.
[340] Romanosky, Telang and Acquisti (2011), pp. 256-262; This is also the aim of the Dutch DBNL which states in its explanatory memorandum that the central availability of the information will stimulate the ability to learn of organizations.
[341] Schwartz and Janger (2007), pp. 913, 971; Mulligan (2007). This discussion is linked to the timing of the notification studied by Bisogni (2015). The faster the disclosure takes place, the more benefits for consumers. I expect this to be equal over significance.
[342] Romanosky, Telang and Acquisiti (2011), pp. 256-262.
[343] Lenard and Rubin (2006).
[344] Mulligan (2007).
[345] Ogut (2005).

Thirdly, the potential liability claim that can follow after a disclosure is a social benefit. Liability results in behaviour that incentivizes organizations to internalize some of the externalities in cyber security. Quite naturally, individuals can only claim damages when a data breach disclosure becomes public and they are aware of it. Liability can even accumulate in class actions.[346]

4.3.3 The social costs

There are also social costs of data breach disclosure. First, individuals and organizations whose data have been breached incur direct costs because they have to spend time and money in order to analyse and mitigate its impact. This might be a minor cost per record, but if hundreds of thousands of records are being breached, the numbers quickly add up.[347] The cost of consumer actions might be greater than expected because consumers can spend several hours of time into their accounts and impose costs on firms by requesting more information on, for instance, new credit cards. For instance, Lenard and Rubin estimate that this cost is $10 per individual.[348] Secondly, an increase in the number of notifications can lead to a decrease in the positive effects of disclosure, because individuals can pay less attention to each individual data breach. Subsequently, the sunlight as disinfectant function becomes less meaningful and eventually all data breaches could just be perceived as noise.[349] I will label this effect as 'notification fatigue'. Thus, notification fatigue does not only impact the benefits of the (least important) data breach, but also has negative externalities

---

[346] Especially in the US, see: Romanosky, Hoffman and Acquisti (2014), pp. 71-104.
[347] For instance consumer spends 10 minutes on gaining knowledge about a data breach, at an 18 euro per hour opportunity cost, a 100.000 record breach can costs society 300.000 euro. These costs are public costs insofar they are not being compensated by the private organization.
[348] Lenard & Rubin (2006). It is more likely to be on the upper side of the spectrum.
[349] Mulligan (2007).

towards other data breaches. All data breaches become less important with the introduction of an additional data breach (through lowering the threshold). Likewise, as soon as more notifications are being made, for example by lowering the notification threshold, the benefits of the additional data breach will decrease and the costs (the negative externality to other data breaches) will increase. Thirdly, organizations may overinvest in security as a result of notifying the data breach. However, this is not expected to be a very significant social cost because in general, organizations have incentives to underinvest in cyber security.[350]

4.3.4 Social costs versus social benefits

Table 22 below displays the public costs and benefits relative to a decreasing notification threshold.

Table 22: Social costs and benefits

Social benefits	**Marginal social benefits relative to a decreasing notification threshold**	**Social costs**	**Marginal social costs relative to a decreasing notification threshold**
Right to know	Decreasing	Administrative costs (individual side)	Minor decrease
Sunlight as disinfectant	Decreasing	Notification fatigue	Increasing
Liability	Decreasing	Overreaction in restricting security	Decreasing

[350] Due to the positive externalities that are present in cyber security (see Chapter 1, Section 1.5.1.)

Marginal social benefits all decrease when less risky data breaches have to be notified. Marginal administrative cost is likely to decrease, because the individual will take more time in reviewing a risky data breach than a less risky data breach. However, the decrease will quickly flatten; because a certain base line of investigative costs have to be made by each individual. Also, overinvestment by organizations will be less likely when less important data breaches have to be notified. Notification fatigue will logically strongly increase when a larger pool of data breaches have to be notified. I assume that the notification fatigue drives overall marginal social costs to increase and the minor decrease of administrative cost and overall minor decreasing effect of overinvestment cannot compensate for that. In sum: there may be positive social benefits from notification but those can be reduced as a result of notification fatigue. To reduce that risk determining the appropriate threshold for notification is crucial (see Section 4.7). For now we assume that a smart threshold will be determined and that disclosure is therefore socially beneficial. That then leads to the following question:

4.4. Will there be Spontaneous Disclosure in the Absence of the Law?

This section discusses whether there will be spontaneous disclosure in the absence of the law. I will assess the private costs and benefits as a consequence of disclosure. Section 4.4.1 will discuss private benefits and section 4.4.2 will discuss private costs. Section 4.4.3 will balance these cost with these benefits.

4.4.1 Private benefits

First, organizations experience a benefit because the disclosure of data breaches allows for the faster mitigation of the impact of the breach. This reduces direct costs. This is especially relevant when consumers need to take actions after the data breach, such as refraining from using

stolen credit card information or using old passwords. Also, a DPA can potentially assist in mitigating the breach by providing advice.

4.4.2 Private costs

Besides benefits, private parties also incur costs when disclosing data breaches. First, there are administrative costs of disclosing data breaches to the affected individuals. However, the big elephant in the room is (perceived) reputation damage. The literature shows that data breach disclosure does have limited single digit (1 or 2%) negative impact market value on the short term.[351] However, research that focussed on the long term suggests that "information security breaches have minimal long-term economic impact".[352] The Target stock price example illustrates the difficulty to point out long-term reputational damage. Target was victim of a very significant data breach in December 2013. Figure 10 below displays the graph of the stock market value of Target. It is impossible to identify the day of the data breach,

---

[351] Reputation damage is usually quantified as the difference in company value before and after the disclosure. Goel and Shawky used such an event study methodology. They measured the market value of the company a few days before and after the notion of a security breach and found a negative effect of on average about 1% of the market value according to Goel and Shawsky (2006), p. 404. Cavusoglu, Mishra and Raghunathan identified through a similar approach an incidental loss of stock prices of 2.1% (Cavusoglu, Mishra and Raghunathan (2004), p. 69). They discuss direct and indirect costs of data breaches, this is a slightly different topic, while this chapter discusses data breach disclosure. Rosati, Cummins, Deeney et al. find that market activity on the short term slightly higher after a data breach announcement (Rosati, Cummings, Deeney et al. (2017), pp. 146-154).

[352] Ko and Dorantes used a matched sample comparison analysis instead of event study methodology to investigate the impact of security breaches on firm performance. These observations about long-term impact should be taken with care, because the effect of the data breach is much harder to disentangle from other exogenous variables and high quality panel data is not available (Ko and Dorantes (2006), p. 13).

as on other trading days stock prices did fluctuate more than during the event in late December. [353]

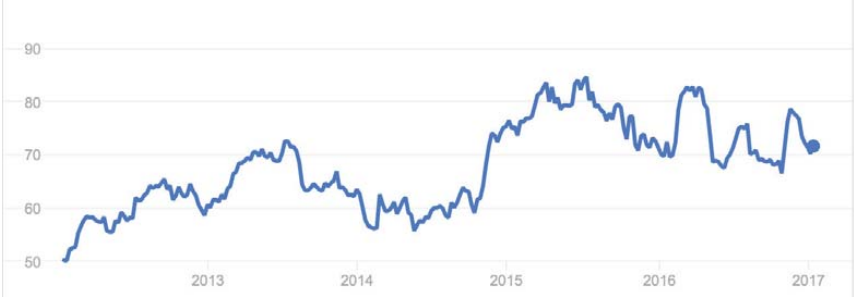


Figure 10: Stock market value of Target Corp.

In practice, the distribution of real reputational costs has long tails. Some organization will suffer no significant long-term reputation damage while other companies will go bankrupt as a result of the disclosure of the data breach. The former group are likely to consist of organizations with a stable customer base that are able to exploit lock in strategies and are too big to fail. A data breach does not reduce the likelihood that consumers buy the product or services of these organizations. The latter group has a small customer base and/or offers products with trust as a core selling point.[354] But possibly, the *perceived* value of reputation damage is more important than the objective value of reputation damage. As a security officer pointed out: "fear of reputation damage … drives organizations to take steps to at least

[353] 'In the days prior to Thanksgiving 2013, someone installed malware in Target's security and payments system designed to steal every credit card used at the company's 1,797 US stores.' See Riley, Elgin, Lawrence and Matlack (2014) <https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data> (accessed 30 March 2018).

[354] Compare for instance the 2017 Verizon data breach with the 2011 Diginotar data breach. The former did not encounter major issues while the latter went bankrupt.

evaluate, if not correct and enhance, security mechanisms".[355] Or consider the following blog post: "Our head of IT Security (of a major telecom) told us once, 'We have one key metric: Don't show up in the Wall Street Journal for a security breach.'"[356]

A third issue is liability. The general logic is that when a data breach becomes public, the opportunity for this public arises to sue organizations. So, notifying data breaches raises the likelihood of liability costs. Romanosky finds that when consumers suffer financial harm, the risk of litigation increases with a factor 3.5.[357] However, there are two drivers that mitigate this effect. First, a well-planned notification strategy for organizations can mitigate liability costs. Liability risks can be reduced when the organization is able to show that it took an effort in notification and reduction of the risk (such as immediate disclosure itself). In the U.S., the likelihood of an organization being sued is six times lower when the organization offers free credit monitoring after the data breach.[358] Second, when a company intentionally conceals data breaches and they nevertheless become public, it can reasonably be expected that the likelihood and impact of claims will be higher. Table 23 below summarizes private costs and benefits.

---

[355] Mulligan (2007).
[356] See the following article on Bruce Schneier's Blog (2009) <https://www.schneier.com/blog/archives/2009/01/state_data_brea.html> (accessed 30 March 2018).
[357] Romanosky, Hoffman and Acquisti (2014). This research is based on US data where the use of liability law is more common than in other jurisdictions.
[358] Romanosky, Hoffman and Acquisti (2014).

Table 23: Summary of private costs and benefits

Private benefits	**Marginal private benefits relative to a decreasing notification threshold**	**Private costs**	**Marginal private costs relative to a decreasing notification threshold**
Mitigation of impact and improvement of security	Decreasing	Administrative costs	Slight decrease
Reduction in reputation damage	Decreasing	Reputational damage	Decreasing
		Additional perceived reputation damage	Decreasing
		Liability cost	Decreasing

Private benefits and costs are strongly correlated with the magnitude of the data breach risk. Private benefits become higher when data breaches that have to be notified are more risky, while decreasing when breaches become less risky. With regards to private costs, in my view these administrative costs of disclosure will decrease slightly, because the administrative procedure to inform customers will take slightly more time when the breach is more significant because it can be expected that individuals demand more information. It is reasonable to expect that the other marginal private costs will decrease relative to a decreasing notification threshold. With regards to absolute numbers, private costs are (perceived as) high and certain, while private benefits are indirect and uncertain. Hence, I assume that private costs of data breach disclosure are higher than private benefits.

Ergo, there are few incentives for a private actor to spontaneously notify data breaches in the absence of the law.[359]

4.5. The Case for the DBNL

Section 4.3 observed that a data breach notification has social benefits, most notably bringing information in the market that serves as a 'Right to Know' and 'Sunlight as disinfectant'. Section 4.4 observed that data breach disclosure most likely imposes a net cost on private parties. There will in most cases not be spontaneous disclosure in the absence of the law. This section examines in whether social surplus is likely to remain, even when net private costs are taken into account and argues that there is a case for regulation. I will also discuss the public cost of enforcing DBNLs.

4.5.1 Is there a case for the DBNL?

Most data breach disclosures impose a cost on private organizations. Above the threshold, the social benefits outweigh the (net) private costs. Within this interval, there is a case for regulation. The social optimal threshold for disclosure will lay a notch higher than in the situation without taking the private optimum into account, because net private losses have to be added to the social costs. The data breaches below the threshold will have insufficient positive effects to compensate for the negative effects and generate a social loss.[360] It becomes quite clear that it is important to give a direction for distinguishing and clarifying the threshold, which section 4.7 will do.

---

[359] Surely, there are data breaches for which private benefits of disclosure exceed private costs. For instance, when there is a (perceived) high likelihood that a breach will be made public by a third party. In such a situation, the difference in reduced (perceived) reputation damage and the threat of liability claims may weigh against disclosure costs.

[360] Lenard and Rubin (2006).

4.5.2 Public cost of the DBNL

There are also public costs of the DBNL. The first is the adoption of the regulation as such. There are costs associated with the discussion and adoption of the regulation in by the EU legislator. These are sunk costs and the regulator can also incur these costs when the regulation is not adopted. There are also costs involved in processing the notifications at the DPA. Furthermore, there are enforcement costs[361] and possible costs involved in offering a digital first aid kit, discussed in the next section.

Table 24: Public costs of a DBNL

Public costs (costs associated with the operation of the legal system)[362]	**Marginal public costs relative to a decreasing notification threshold**
Adoption costs	Sunk costs
Costs of DPA	Stable
Costs of enforcement	Stable for general enforcement, up to threshold violation specific enforcement
Costs of the digital first aid kit	Stable

When I add the public costs to the new social optimum, the socially optimal threshold becomes higher.

[361] Polinsky and Shavell (2005); Oded (2011); Stigler (1970), pp. 526-536).
[362] "To amplify, the private cost of a suit is less than the social cost of a suit, for that includes the injurer's costs as well as the public costs (those costs associated with operation of the judicial system)." Shavell (1999), p. 100

4.6. Will the EU DBNL Sufficiently Induce Organizations to Notify?

Section 4.3 argued that disclosure is socially beneficial for a certain area of data breaches (up to the threshold). Section 4.4 concluded that, for the majority of those data breaches, there will be insufficient incentives for spontaneous disclosure by private parties. Section 4.5 argued that there is a case for regulation, because these social benefits are higher than private costs, provided that the benefits of regulation outweigh the public costs of regulation. The question this section aims to address is whether the EU DBNL will sufficiently induce organizations to notify those data breaches for which disclosure is socially beneficial.

4.6.1 The administrative fine

The administrative fine is the main design parameter that induces organizations to notify within Articles 33, 34 and 84(4) the DBNL. Especially Article 84(4) GDPR gives DPAs this stick.[363] DPAs are granted the power to impose an administrative fine of €10,000,000 or 2% of the undertakings turnover, whichever is higher, in case of non-compliance with the regulation.[364] The fine can be imposed when an organization conceals a data breach or does not notify in due time. The administrative fine has several theoretical advantages. First, the fine has a multiplication effect. The fine has an effect once imposed as well as the threat of the effect. This threat can be executed multiple times once organizations comply. This induces them to stay compliant. Thus, when the sanction is set at a deterrent level that forces all organizations to comply, the sanction itself is costless, because it does not have to be executed. In such a situation only the threat suffices.[365] Moreover, even

---

[363] Nieuwesteeg (2014). The majority of the DBNLs in the world apply sticks in order to deter non-compliance.
[364] Article 83 (4) GDPR.
[365] Dari-Mattiaci and De Geest (2010), pp. 341-392; compare the discussion in section 4.4.2 on perceived reputation damage.

if the fine has to be imposed, the fine itself is considered to be a socially costless transfer of money (contrary to other sticks such as imprisonment).[366] Last, higher sanctions allow for lower levels of enforcement to keep an identical level of deterrence. The high sanctions in Article 84(4) GDPR consequently could save enforcement costs.

However, the high fine in Article 84(4) GDPR also has several disadvantages. For small organizations, the maximum de facto fine will be lower because a high fine will go beyond their solvency.[367] Next, high sanctions can lead to over- and under deterrence when the perception of the likelihood of detection differs from the actual likelihood of detection.[368] This phenomenon especially occurs when there is a low likelihood of detection. To be concrete, organizations could be incentivized to notify data breaches that are not subject to mandatory notification (because they do not result in a risk for individuals) just because they want to be 'on the safe side'. This assumes that the organizations do not have exact information about the threshold, which is reasonable to expect. In a situation of overdeterrence, organizations will disclose data breaches for which disclosure is not socially beneficial and this will result in a social welfare loss. Furthermore, a high administrative fine can incentivize organizations not to detect data breaches.[369] Closely connected, individuals show risk seeking behaviour when facing losses. This

---

[366] Polinsky and Shavell (2005).
[367] Also, in practice, it is likely that most actual fines will be lower than the maximum, lowering their deterrent effect. Article 83(2) specifies several circumstances of the case that have to be taken into account for the actual determination of the fine, such as negligence and mitigation measures.
[368] Polinsky and Shavell (2005).
[369] Polinsky and Shavell (2006).

undermines the deterrent effect of high fines.[370] A last disadvantage of the (high) administrative fine is that it will punish the organization itself (and thus the shareholders and customers) and not the people responsible for concealing the data breach itself.[371]

4.6.2 Enforcement of the fine

The administrative fine of the DBNL is high, but the expected value of the administrative fine is the magnitude of the fine times the likelihood of detection. Hence, its deterrent effect largely depends on the ability of the DPA to effectively enforce at acceptable social cost.[372] What be should the level of deterrence? The level of deterrence should exceed the net private cost that organizations incur when disclosing a data breach.[373] This private cost is not static but varies across organizations and will also be different per data breach. Section 4.4 concluded that private costs are (perceived as) high and certain, while private benefits are indirect and uncertain. Hence there is a significant gap between private costs and benefits that should be closed by an appropriate deterrent effect of the DBNL in order to induce organization sufficiently to notify.

The appropriate level of deterrence can be accomplished through enforcing the law and by increasing the likelihood of detection. The GDPR does not give further instruction on how to enforce the law apart from the statement that enforcement should be 'strong' according to

---

[370] Kahneman and Twersky (1979).
[371] Polinsky and Shavell (2005).
[372] Dari-Mattiaci (2010) and Becker (1968), pp. 169-217. According to the theory of deterrence, the strictness of the stick equals the magnitude of sanction stick multiplied by the probability of detection.
[373] See Section 4.4

Recital 7. This section will discuss several possibilities for enforcement of the EU DBNL.

General enforcement concerns auditing random organizations to investigate whether they comply with the DBNL. General enforcement is characterized by the fact that it does not depend on the number of individuals who actually commit harmful acts.[374] An example of the current Dutch DBNL that will be replaced by the EU DBNL illustrates that general enforcement will be costly.[375] Suppose the Dutch DPA wants to achieve a likelihood of detection of 10% and it will be able to successfully find a data breach in half of the cases where one has occurred.[376] Then it must audit 20% out of the total number of 132,000 organizations in the Netherlands.[377] No more than 20 organizations per year can be audited by one FTE.[378] Hence, to audit 20% one needs 1320 FTE. Given an average annual total cost for skilled personnel of €100,000, the regulatory costs of enforcement rise to €132,200,000 per annum. In 2017, the total capacity of the Dutch DPA in Netherlands is 72,5 FTE, that only can be partially deployed for enforcement.[379] Suppose that 25% of the Dutch DPAs total capacity (18,125 FTE) can be devoted to general enforcement of the law. This results in an actual likelihood of detection of around 0,27%. In addition, general enforcement causes significant administrative costs for the organizations that are subject to an audit. Many of them have nothing

---

[374] Oded (2011).
[375] Laube and Böhme (2014), p.7.
[376] I assume 50% likelihood of detection because an organizations can quite easily actively conceal data breaches by for instancing removing log files about the breach.
[377] According to the Dutch estimation when the DBNL was adopted;
[378] Assuming 10 days FTE work for an intensive auditing procedure with
[379] See <www.autoriteitpersoonsgegevens.nl>(accessed 30 March 2018). The Dutch DPA also has other tasks.

to hide and have to devote time and money to the auditing procedure which aggravates the social cost of general enforcement. Ergo, in my opinion, general enforcement is not a socially efficient instrument to increase the deterrent effect of the DBNL.[380]

Ex ante risk based auditing is a more efficient means of enforcement. This approach starts with prioritizing sectors or organizations that are most likely to violate the law. In the US, for instance, healthcare and financial institutions have been subject to data breaches relatively more often than other sectors.[381] In addition, DPAs can prioritize their enforcement efforts on those sectors where the disclosure of data breaches is most likely to lead to the highest social welfare increase. Logically, ex ante risk based auditing reduces costs because the average likelihood of detection is likely to increase per audit. However, this should be weighed against the cost of ex ante efforts in determining the risk and the possible perverse incentives of organizations in low risk sectors. When these costs are kept sufficiently low, for instance through diffusing information about risk assessments across the EU, risk based auditing is preferable over general enforcement. However, a labour intensive auditing procedure is likely to remain.

Violation specific enforcement entails that the DPA enforces violations of the EU DBNL that are discovered by third parties, such as white hackers, the media and individuals affected by the data breach.[382] Verizon suggests that 70-80% of the data breaches that reach the public are discovered by third parties. Unfortunately, this does not mean that

---

[380] Laube and Böhme (2014), p.7.
[381] Edwards, Hofmeyr and Forrest (2015).
[382] Verizon (2012). When the risk of third party disclosure is very high, it will have an identical effect as intense enforcement, but I assume that this is not the case. ; White hackers penetrate security systems in good faith in order to check security.

of all data breaches, 70-80% will be discovered by third parties. Hence, we cannot exclusively rely on violation specific enforcement when only a small proportion of data breaches reaches the public. Suppose that 10% of the organizations experience a data breach. When 1% of the data breaches reaches the public, 0.7-0.8% will be discovered by third parties and 0,2-0,3% will be disclosed by the organization itself. For violation specific enforcement, it is necessary that third parties have sufficient incentives to notify the DPA. Consequently, they must be fully compensated for their cost in notifying the DPA.[383] Ideally, they must solely notify the DPA, because the DPA needs to determine whether disclosure to individuals is socially beneficial. Otherwise, inducing third parties to discover data breaches could contribute to notification fatigue. Similar to the stimulation of third party disclosure, the DPA could also stimulate data breach notification by whistle-blowers by compensating them for their private losses. The fact that violation specific enforcement capitalizes on the efforts of third parties or whistle-blowers leads to the conclusion that it could be a more socially beneficial type of enforcement than ex ante enforcement, because the DPA does not have to engage enforcement activities with an uncertain outcome. On the downside, the level of deterrence will fully depend on the capacity of third parties to discover data breaches.

4.6.3 The digital first aid kit

Section 4 demonstrated that there will not be spontaneous disclosure in the absence of the law. Also a mere data breach notification obligation without additional incentive schemes will not yield spontaneous disclosure. The previous section discussed the deterrent effect of the stick in the EU DBNL. It is likely that, although the lawmaker is fully informed, he is not able to set deterrence at such a level that it will induce organizations to notify at socially acceptable

[383] De Geest and Dari Mattiaci (2013), pp. 341-492.

cost. This is related to the fact that the ex ante enforcement of administrative sanctions in the DBNL is costly and that ex post enforcement depends severely on third parties. Theoretical and empirical evidence[384] supports this statement, although there is limited attention in the literature for the effect of the unprecedented high administrative fines of the EU DBNL in the GDPR. The question arises whether there are other options on the table that can further induce organizations to comply with the DBNL at reasonable social cost. In this and the next section, I will focus on those options that do not involve a significant alteration of the GDPR. Instead, I focus on more feasible incentive schemes, which can be implemented within the scope of the law.[385]

When it is expected that most organizations will conceal data breaches or will refrain from detecting them, rewarding compliance (offering carrots) may have lower costs than sanctioning and detecting violators

---

[384] Boehme (2015); Nieuwesteeg (2014). Also there is anecdotal evidence that there is undercompliance in the case of the Dutch DBNL, see for instance Rob de Lange (2017): <https://fd.nl/economie-politiek/1185463/veel-bedrijven-negeren-wet-meldplicht-datalekken> (accessed 30 March 2018, Dutch).

[385] For instance, criminal penalties are not imposed by the EU. However, the GDPR allows certain administrative fines to be fined as a criminal fine because of the legal system of some of the MS and sometimes the MS are free to choose the type of penalties when it is not being harmonized (Recital 151 and 152 GDPR). This is also related to the competence of the EU (Graig and the Burca (2015)). Criminal penalties have two advantages. In the first place, they hit certain natural persons directly. Secondly, a criminal penalty is insensitive for the financial situation of an individual (the limited individual wealth issue of administrative sanctions is not of concern) when the criminal penalty is non monetary. (Polinsky and Shavell (2005)) Another example is liability. Liability can potentially be increased when an organization is non compliant and decreased when an organization is compliant.

(using sticks).[386] The single carrot that I will discuss is the possibility of the DPA to provide the organization with specific tailored information that can reduce the impact of the data breach and reduce reputation damage, a 'digital first aid kit'. [387] In other words, if organizations know that the DPA has essential information that will assist them in being resilient concerning the data breach, they will have additional incentives to disclose. This section discusses its opportunities, drawbacks and prerequisites.

Opportunities. Carrots work best in situations when organizations have different options in complying.[388] This is the case in complying with a DBNL. The disclosure of more risky data breaches will have a higher cost than the disclosure of less risky data breaches. The advantage of the carrot, the digital first aid kit, is that it can offer greater rewards for more risky data breaches in the sense that for more risky data breaches the value of useful assistance is also higher. Furthermore, the digital first aid kit benefits social welfare because it propels the diffusion of information in cyber security. For this, it is necessary that the costs of the stimulation of information diffusion remain lower than its benefits, which can be achieved through cooperation between national DPAs and automatization of the first aid kit regarding its internal decision

---

[386] Wittman has analysed the role of administration costs. He argued that if most organizations obey the law, punishing violators is cheaper than rewarding compliers and vice versa (Wittman (1984), pp. 57-80).
[387] Another possible carrot is the reduction of liability for data breaches when a data breach is notified in due time. However, liability is largely regulated by private law within the MS and therefore does not fall within the scope of the GDPR. Also the DPA could offer a monetary compensation for the administrative costs in notifying a data breach. However this can be costly and can have perverse and distortive effects and therefore I will not discuss this option.
[388] De Geest and Dari-Mattiaci 2013, pp. 341-392.

making process about which information to give to which organizations.[389]

Drawbacks. Carrots have more transaction costs than sticks, because the carrot has to be carried out each time an organization complies, and the stick only has to be executed when an organization does not comply with the law.[390] However, this effect is partly mitigated by the fact that high enforcement costs are likely to prohibit the lawmaker from setting deterrence at such a level that it will induce organizations to notify at socially acceptable cost. To put it simple, there will still be many violators because the deterrent level cannot be set sufficiently high. Moreover, the specific carrot advocated, the digital first aid kit, has additional social benefits that justify some cost in their execution. A second drawback is that carrots can have distortive effects on the equal distribution of goods when not applied uniformly.[391] Indeed, some organization will experience more benefits than others and this is something to be reckoned with in the execution of the carrot.

Prerequisites. First, it is indispensable that the DPA invests in becoming a hub and knowledge centre for data breach information diffusion. It is required that the DPA is able to quickly categorize the data breach and estimates whether the organization affected needs assistance and which information is relevant to provide. National DPAs can leverage upon the EU wide application of the GDPR.[392] This requires that the DPA can quickly make an estimation based on the nature of the data breach and the mitigation measures to assess which lessons learned from other data breaches in their database should be transferred to the

---

[389] Cetin, Gañán, Korczyński et al (2017).
[390] Dari Mattiaci and de Geest (2010).
[391] Wittman (1984), pp. 57-80.
[392] Already stressed in Articles 60, 61 and 62 of the GDPR.

organization making the data breach. An import aspect is the implementation of a continuous feedback loop that tests whether the information was in fact valuable for the organization. Advanced data analytics is necessary here. Secondly, in order to achieve the desirable network effects of information diffusion, enforcement and investments must be above average in the early stages of the application of the GDPR. The digital first aid kit solely functions when information about best practices and mitigation measures is already there. Hence, this information needs to be obtained first without the digital first aid kit as a carrot. This necessitates excessive enforcement in the early stages of the GDPR in order to generate the necessary data breach notifications to propel the network effects.

4.6.4 The expressive function of the DBNL

Section 6.1 showed that enforcement based on sticks is costly. As security economists Laube and Böhme conclude after modelling mandatory data breach disclosure: "Security breach notification laws *without* security audits, regardless of the level of sanctions, cannot incentivize firms to report security breaches to authorities, given positive disclosure cost."[393] However, despite the lack of positive incentives to do so, still data breaches were notified in the Netherlands and the US without substantive enforcement efforts.[394] The fact that organizations have disclosed data breaches despite clear incentives not to do so can be attributed to the likelihood of detection through third party enforcement. However, it could also be attributed to the expressive function of the law, which is another scheme that affects the incentives of organizations. Through its expressive function, the law

---

[393] Laube and Böhme (2014), p 19.

[394] Nieuwesteeg (2014) and for instance Van der Beek (2016): <https://www.computable.nl/artikel/nieuws/security/5716753/250449/autoriteit-registreert-700-meldingen-datalekken.html> (accessed 30 March 2018, Dutch).

affects behaviour by internalizing social norms.[395] The basic premise is that organizations can gain utility from the fact that they are compliant with law.[396] Stimulating the expressive function is a socially cost efficient way to induce private parties, as there are close to zero variable social costs involved. The EU DBNL can have a strong expressive function based on its two core societal goals.

Right to know of individuals. The expressive function of the EU DBNL on protecting the fundamental right to the protection of personal data is already present. It is embedded in the broader GDPR that aims to execute the fundamental rights to the protection of personal data. The expressive function lies in the fact that most people will agree that protecting fundamental rights is something worth pursuing, and will be more compliant with such legislation *ceteris paribus*.

Sunlight as disinfectant and contribution to cyber security. The EU DBNL can have an expressive function in the fact that data breach disclosure can help others and contributes to overall cyber security. Apart from the directly beneficial digital first aid kit, discussed in the previous paragraph, the DPA could share certain information and best practices of cyber risk management pro-actively. For instance, the DPA could build (anonymized) metrics about data breaches.[397]

---

[395] Cooter (1998), pp. 585-608; Cooter (2000), pp. 1577-1601; see also Ayres and Braithwaite who distinguished profit maximization (the logic of consequences) and morality (the logic of appropriateness) as main motivations for compliance (1992).
[396] Parisi (2013).
[397] Building metrics about cyber data is one of the key challenges in cyber security economics.

4.6.5 Summary

Table 4 below displays the various incentive schemes to induce organizations to notify and their public costs.

Table 25: Incentive schemes and their public costs

Public costs	Incentive scheme	Marginal public costs relative to a decreasing notification threshold
Almost zero public costs	Threat of administrative fine of €10,000,000 or 2% of the undertakings turnover,	Stable
	Expressive function of the law	Decreasing
Low public costs	Violation specific enforcement	Stable
Medium public costs but compensated by social benefits	Digital first aid kit	Decreasing
Medium public costs (depends on intensity)	(Limited) Ex ante risk based auditing	Stable
High public costs	General enforcement	Stable

4.7. Which Disclosure Threshold will Contribute to Social Welfare?

Section 4.6 discussed whether the EU DBNL sufficiently induces organizations to comply with the law. If we suppose that a smart mix of incentives can indeed sufficiently induce sufficient organizations to comply with the law, then the disclosure threshold determines the

social benefit (or when set wrongly, the social cost) of the EU DBNL.[398] This section discusses the disclosure threshold for DPAs and individuals.

4.7.1 The disclosure threshold for notification to DPAs

The GDPR defines the threshold for notifying to the DPA as those data breaches that result in a 'risk to the rights and freedoms of natural persons'.[399] How should this threshold be interpreted? And should there be a difference in notifying to the DPA and individuals? To begin with the last question: the difference between in threshold notification to the DPA can be explained quite easily because the total social costs of doing so are only a fraction of notification to individuals. The organization that notifies has limited costs in providing the DPA the necessary information (compared with communicating to an often large group of individuals) and the DPA has limited costs in processing the information.[400] Moreover, it can already provide the organization with its 'digital first aid kit', which generates social benefits. Social costs such as administrative costs of the individual and notification fatigue do not manifest when solely the DPA has to be notified. Hence, the threshold for notification to the DPA should be fairly low, especially because the DPA itself might be better able to judge whether an additional notification to individuals is necessary from a social welfare perspective.[401]

---

[398] See Section 4.2 for a discussion regarding the disclosure threshold in the text of the regulation.
[399] Article 33 GDPR
[400] See Section 4.5.2.
[401] And it has the power to do so ex Article 34(4) GDPR.

4.7.2 The disclosure threshold for notification to individuals

In the case of notification to affected individuals, the GDPR raises the threshold in Article 34 by adding that in this case the risk to the rights and freedoms of natural persons should be 'high' (Article 34).[402] This incremental threshold can be explained, because the social costs of notification to individuals are much higher. First, data breach disclosure to individuals in general results in a larger net private loss because of reputation damage, higher administrative costs of disclosure (compared to notifying solely to the DPA) and the potential liability costs.[403] Secondly, there are also significant social costs of data breach disclosure such as administrative costs of processing the notification by affected individuals and notification fatigue.[404] On the other hand, notification to individuals generates most of the 'right to know' and 'sunlight as disinfectant' social benefits.[405] The DPA should specialize in estimating in which situations costs outweigh benefits and give clear guidelines and examples on when an organization should notify and when not. A higher threshold for notification to individuals in combination with a relatively low threshold for notification to DPAs is preferable. In case that an organization wrongly interpreted that it should not notify individuals according to the high threshold, Article 34(4) allows the DPA to correct this underestimation and may require that the organization notifies individuals anyway. This reduces the likelihood that data breaches are disclosed that are not socially beneficial.

---

[402] See Section 4.2.
[403] Section 4.4.2.
[404] Section 4.3.3.
[405] De Hert and Papakonstantinou (2016), pp. 179-194: compared to earlier versions of the GDPR, the notification requirement for consumers is a 'notch' higher, as former versions did not include the requirement that the risk should be high.

4.7.3 Smart Thresholds

Under the current regime, there are basically two actors that can decide whether to notify data breaches to the public, the data controller itself ex Article 34 GDPR and the Data Protection Authorities (DPAs) ex Article 34(4) GDPR. The analysis above describes the optimal disclosure threshold within the scope of the law for both actors. When we allow ourselves to think slightly beyond the current Articles 33 and 34 of the GDPR, other solutions emerge for a 'smarter' threshold.

There are strong arguments for an intensified role of the DPA in the notification procedure. This is related to the fact that DPAs can build up expertise in determining the threshold, being a repeat player contrary to individual data controllers which are 'one-shotters'.[406] The approach followed in the GDPR to rely primarily on disclosure to the DPA can therefore be understood, precisely since the potentially averse consequences of notification (notification fatigue and reputational damage) will especially arise in case of notification to individuals. One could even raise the question whether a notification to individuals does have an added value. Does a system of a notification to the DPA, whereby the DPA according to Article 34(4) GDPR decides whether information to the general public is necessary, not suffice? In most cases it probably does. However, there may be situations of data breaches where a mere notification to the DPA may not suffice, for example because potentially high damage could result to individuals if no immediate action is taken. The notification to the DPA could then slow down further action, especially because it is not known whether the DPA will indeed inform the public. Therefore, although notification to the DPA has priority, for cases where the data

[406] Galanter (1974).

breach could result in high risks, it is still important to have a subsequent duty to notify individuals as well.

A more intensified role of the DPA also complements the discussion on the 'digital first aid kit' in Section 4.6.3. When DPAs develop expertise to provide assistance to data controllers on mitigating damage, it can reasonably be assumed that they also have a better position in determining whether notification to individuals is social welfare increasing. The question is thus which decision making model should form the basis for the DPA to decide whether notifications that they received from data controllers should also reach the public, given the social cost and benefits of such a notification. The following questions are relevant:

1. Is there direct action needed for individuals? When direct action is needed, the data breach should be notified in any case, insofar the benefits of these actions exceed the administrative costs at the side of the individual.
2. What is the impact on the rights and freedoms of individuals of the data breach? Can we distinguish certain categories such as low, medium and high impact breaches?
3. When does notification fatigue kick in? Would it be desirable to make the notification decision contingent upon the previous amounts of notifications to an individual? Here it possibly useful to use insights from the fields of psychology and behavioural economics.

4.8. Concluding Remarks

From May 26 2018 onwards, the EU finally has a general data breach notification law as part of the GDPR. Most organizations will not spontaneously disclose in the absence of a regulation. The simple reason is that the private costs of notification are higher than the social

benefits. This indeed necessitates regulation from a social welfare perspective, provided that solely data breaches that surpass a threshold are disclosed to the public. I conclude that the two main challenges of the EU are to sufficiently induce organizations to notify and to set the notification threshold at a socially acceptable level. Regarding the former, I argue that solely relying on deterrence will potentially be very costly or result in a limited likelihood of detection, even if ex ante risk based auditing or ex post violation specific enforcement are taken into account. It is hard to predict the effects of the high administrative fine provided for in the GDPR. It could either lead to under-deterrence given the low probability of detection or to over-deterrence leading to too many notifications and thus to notification fatigue. The precise direction may depend upon the risk attitude of the data controllers and on their (subjective) assessment of the probability of detection. But both risks point at the limitations of a deterrence approach.

I urge the DPA to look at carrots and the expressive function of the law as alternative incentive schemes. Especially the digital first aid kit can be a promising additional incentive for organizations to comply, provided that DPAs developed themselves as a centre of expertise in mitigating data breaches. Regarding the latter (the optimal level of the threshold) my analysis clarified that data breach disclosure can be a costly exercise from a social welfare perspective. Especially notification fatigue and administrative costs of affected individuals negate social benefits when large amounts of insignificant data breaches are being disclosed to the public. Hence, that threshold for notifying to individuals needs to be fairly high and clear-cut. The threshold for notifying the DPA can be much lower.

Unfortunately there is little empirical research in this area. There are some data on data breaches, but for example little is known on the

effects of DBNLs. The entire EU DBNL is therefore largely based on assumptions on how data controllers will react to the DBNL given the particular sanction regime. We already indicated that even theoretically it is difficult to predict the effects of the regime as it strongly depends on specific assumptions. Those may be crucial to determine the effectiveness of the DBNL. Once the DBNL has been put in place (in May 2018), it will be interesting to examine its effects on the basis of empirical studies. Before that time, the predictions on the effects of the DBNL remain largely based on theory.

The EU DBNL can be a welfare-enhancing piece of legislation provided that it will be enforced wisely and executed by the national DPAs. Of course the social effects of the DBNL depend upon the actions taken by the DPAs after they have received the information on data breaches. If by the end of the day notifications would merely end up in a digital drawer at the DPA and no further action is taken to promote cyber security, then obviously the entire DBNL would only be an extremely costly exercise without any social benefits as far as improving cyber security is concerned. This points at the crucial role to be played by the DPA to make the EU DBNL a success.

PART III:

Industry

5. INTRODUCTION TO PART III: THE POTENTIAL OF RISK SHIFTING

5.1. Introduction

Where Part I focused on the role of universities and Part II focused on the role of governments in stimulating information diffusion in cyber security, this third part focuses on the role of industry. Industry has the contractual freedom that enables the development of techniques that can lead to innovative products or services. Risk shifting is such a technique. When designed properly, risk shifting increases incentives for information diffusion. Traditionally, two types of risk allocation are taken into consideration by scholars in cyber security, namely individual management by the firm[407] and the (partial) transfer of risk to an insurer: cyber insurance.[408] Part III will address these two alternatives in the light of their ability to shift risk in an effective manner in cyber security and stress the need for exploring a third way of managing cyber risk, namely by sharing them amongst firms without the interference of an insurer (cyber risk pooling).

Accordingly, this first chapter within Part III will provide a brief introduction into the theory of risk shifting. Chapter 6 will subsequently focus on risk transfer (insurance) and Chapter 7 will focus on risk sharing (pooling). This chapter is structured as follows. Section 5.2 will address why and when there is demand for risk shifting in the market. Section 5.3 will describe the three forms of risk allocation.[409] Section 5.4 will discuss the social benefits of the two risk

---

[407] Rowe & Gallahar (2006).
[408] Biener, Eling and Wirfs (2015, pp. 131-158).
[409] Risk shifting and risk allocation will be used interchangeably in this Part. However, strictly speaking the allocation of risk to the individual (individual management) is not a form of shifting risk.

shifting techniques relative to individual risk management. Finally, section 5.5 will disclose the storyline of Chapters 6 and 7.

5.2. Demand for Risk Shifting

Before addressing the three alternatives for risk allocation it should be addressed why a demand for risk shifting is created in the first place. In the literature two foundations for risk shifting are distinguished.

5.2.1 Reducing risk (risk aversion)

A first, and the most traditional economic approach, is to consider risk shifting as a remedy for risk aversion.[410] Individuals (and organizations[411]) may have an aversion against risk that occurs with a low probability and high damage.[412] Given wealth restraints and the decreasing marginal utility of wealth, individuals suffer disutility from the risk of being exposed to the possibility of losing a large amount of wealth. Since risk aversion creates disutility for individuals and organizations, social welfare increases if risk is removed from individuals with risk aversion.[413] Hence, risk averse actors are willing to pay more than the expected loss to reduce or remove the risk.[414] However, the degree of risk aversion depends on the type and the size of the risk, the possibilities of risk diversification and on the wealth of the individual concerned. With regards to the latter, consider the

---

[410] See Shavell (2004, pp. 258-259).
[411] Koller, Lovallo and Williams (2012) <http://www.mckinsey.com/client_service/corporate_finance/latest_thinking/~/media/D2CF206B82C34F1FBB87FE591599A958.ashx> (accessed 30 March 2018). Especially SMEs, which are the topic of the empirical research in Chapter 6, are relatively small and have limited ability to effectively diversify, they can be assumed to be risk averse.
[412] See Wagner p.377, in Faure (2009); Zweifel and Eisen (2003), p.59; Shavell (2004), p. 258.
[413] Shavell (2004, p. 259).
[414] See Wagner p.377, in Faure (2009).

following example: an individual who only possesses €50,000 may be highly averse against a 1% risk of losing €40,000. However, if the same individual would possess several millions there would be almost no risk aversion and hence also no demand to hedge particular risks. This starting point is quite important as it explains that the demand for risk shifting by firms exposed to cyber security will depend upon the type of risk (low probability, high damage or rather the reverse) and on the individual wealth situation of the firm concerned.

Therefore, the demand for risk shifting will be high in a situation where the risk to which the firm is exposed is relatively high (in the sense that a high damage can occur when the risk materializes) and when the individual wealth of the firm is limited. The latter may more particularly be the case when the potential damage if the risk materializes would be higher than the wealth of the firm. This simple economic logic is also related to the fact that risk shifting is not a costless exercise. Therefore, a significant willingness to pay for risk shifting will only occur in case of strong risk aversion, i.e. for relatively high risk (high damage if the risk materializes) and for less wealthy firms. This also shows that the attitude to risk and the related demand for risk shifting is not binary (in the sense of all or nothing), but of course has a gradual nature. The latter may more particularly be important since some techniques of dealing with risk (like individual risk management) have lower costs than others (for example insurance).

5.2.2 Reducing transaction costs

In addition to this first, classic, reason for risk shifting (and more particularly for insurance) based on risk aversion, also other reasons have been advanced in the literature. It has for example been argued that insurance could reduce transaction costs. Operators often wish to benefit from services offered by insurance companies. Insurers offer

the services of administrating claims at much lower costs than corporations would be able to do themselves. This is related to the specialization of insurers in claims handling, but also to economies of scale. The advantage for traders is that the contractual conditions in the insurance policy (aiming at the reduction of moral hazard) in fact replace the need for traders to contract in detail, for example, concerning the allocation of risk.[415] This explains why there is a demand for risk shifting also by actors who suffer no risk aversion.[416]

The actors that seek risk shifting in the case of cyber security are mostly commercial operators and not individuals. Corporate actors are, differently than individuals, often assumed to be relatively risk neutral, especially when they are well-capitalized. However, precisely due to the specific systemic uncertainties of cyber security risk there may be a demand for shifting cyber risk, even for corporate actors.[417]

5.3. Three Forms of Risk Allocation

5.3.1 Individual management

The status quo of individual risk management means that the individual firm will deal with the cyber security risk itself, for example through security by design, and ex post risk mitigation.[418] Individual risk management is therefore not a tool of risk shifting, but rather, as it is sometimes wrongly called, a form of self insurance.[419] Based on the simple economic logic I just presented, it may be clear that individual

---

[415] Skogh (1989).
[416] Faure and Porrini (2017).
[417] See also Chapter 1, Section 1.3.5.
[418] See the resilience strategies in Chapter 1, Section 1.3.6.
[419] Self insurance is not insurance as there is no risk spreading, but usually it just concerns a reservation for future losses. See Faure (2004), pp. 457-458.

risk management will be attractive for relatively small cyber risk (i.e. low damage if the risk materializes) and also for wealthy firms. To take an example unrelated to cyber security: most large oil and gas producers (often referred to as the majors) have no demand for insurance to cover risk related to the damage caused by offshore facilities for the reason that they can cover the risk themselves.[420] For that reason British Petroleum (BP) did not have insurance cover when the mobile offshore oil rig Deepwater Horizon exploded on April 20, 2010, causing massive damage. Also Target Corp., which experienced a major data breach in 2013, only had cyber insurance cover for 36%.[421] For other firms, the potential impact and liability of cyber risk could go well beyond their own solvency.[422]

However, individual risk management has its limits. In case of individual risk management the disutility caused by risk aversion is not remedied. Moreover, the individual organization party has no or little incentives for cyber security information diffusion.[423] In case of individual investment in prevention, the externality problem continues to exist in the sense that there may be underinvestment or overinvestment by the private party relative to the social optimum.[424] As I discussed in the first chapter of this study, in a situation with correlated risk, the firms' security depends on the behaviour of others and vice versa. Hence, the incentives for security investments may

---

[420] Faure, Liu and Wang (2015) pp. 356-383.
[421] See Insureon (2015) <http://www.insureon.com/blog/post/2015/03/24/how-much-does-your-cyber-liability-insurance-cover.aspx> (accessed 30 March 2018).
[422] Faure and Hartlief (2003), online publication 28 June 2003, doi:10.1787/9789264102910-en.
[423] Provided that other means to stimulate information diffusion, for instance the data breach notification obligations discussed in the previous chapter, are not deployed.
[424] Chapter 1, Section 1.5.1.

even be perverse as third party behaviour possibly negates or increases the payoffs the firm receives from its own investment in protective measures.[425]

5.3.2 Cyber insurance

Insurance is a technique to provide cover for risk aversion through the (partial) transfer of risks (which are low probability, high impact risks) to a third party in return for a premium.[426] This transfer is a remedy for risk aversion when firms are more risk averse than insurers, and the costs of the transfer do not outweigh the benefits.[427] 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 the large numbers' reduces risk for the insurer. This risk aggregation enables more accurate predictions of the expected losses.[428] However, the premium paid to an insurer will often be substantially higher than the expected value of the risk (the probability multiplied with the damage). The reason is that insurers may add a risk premium in case of uncertainty or insurer ambiguity;[429] the other reason is that insurance involves transaction costs (referred to as loading) to be able to run the insurance company. That again explains the gradual nature of the demand for insurance: if risk aversion is high, the firm may still have a demand for insurance (even though the premium is higher than the objective value of the risk). If the risks are not considered to be extremely high, the organizations may not have a demand for

---

[425] Kunreuther and Heal (2003), pp. 231-249.

[426] Mukhopadhyay, Chatterjee and Saha et al (2013), pp. 11-26.; Shackelford (2012), pp. 349-356.

[427] Kesan, Majuca and Yurcik (2004).

[428] Priest (1987), pp. 1521-1590

[429] Hogarth and Kunreuther (1985).

insurance, or only demand cover for higher layers of risk. Cyber insurance products have emerged on the market since the early 2000s.[430] Currently, around 10% of European firms have purchased cyber insurance, and this number is probably an order of magnitude lower for SMEs.[431] Chapter 6 will empirically analyse cyber insurance contracts for SMEs.

5.3.3 Cyber risk pooling

In the early days of mankind risk pooling was a first rudimentary form of insurance. If somebody's vessel was destroyed, neighbours committed to help rebuild it, while at the same time, the owner of the vessel committed to rebuild the neighbour's vessel in case of destruction.[432] Chapter 7 takes us back to these forms of risk sharing, by examining the concept of cyber risk sharing, also called 'pooling'. Cyber risk pooling is risk sharing between organizations without transferring this pool to a third party like an insurer.[433] A risk pool brings them together, or brings in an expert to help them, which is commonly called a managed security service (MSS).[434] In doing so, a risk pool is also capable of reducing risk.[435] Buhlmann defines pooling as follows:

> "Any formal mutual agreement among n companies that, operating as an entity, (1) accepts the responsibility for paying for an input; (2)

---

[430] Luzwick (2001), pp. 16-17; Kesan, Ruperto and Yurcik (2004).
[431] Willis (2013) estimates that 6-10% of the US firms purchased cyber insurance.
[432] Jus (2013), p. 7. Risk sharing was already applied between various operators in the middle ages exposed to similar risk. See Skogh (2008), pp. 297-305.
[433] Cyber risk pooling is also called a form of mutual insurance, or risk sharing, or the formation of risk clubs.
[434] Zhao, Xue and Whinston (2013).
[435] Buhlmann and Jewell (1979), pp. 243-262.

> charges companies for accepting the input, according to the agreed-upon rule for sharing risks; (3) operates on a zero-balance conservation principle."[436]

To the best of my knowledge, risk pools currently do not exist in cyber security. There would be some notable differences with an insurance pool. Risk pools in other sectors are usually smaller than cyber insurance pools, in order to exploit one of their main competitive advantages, the ability to execute efficient and effective mutual monitoring.[437] Whereby a cyber risk pool would have a plausible size of 20 participants, a cyber insurance pool could have over thousand participants. This means that within a cyber pool, risk reduction is lower than in an insurance pool.

5.4. Social Benefits of Risk Shifting

This section will discuss the social potential of the two risk shifting techniques. Section 5.4.1 will discuss the potential in stimulating information diffusion and section 5.4.2 will discuss the potential in reducing risk aversion. The drawbacks of risk shifting (and possibilities to mitigate them) will be discussed in Chapters 6 and 7.

5.4.1 Stimulating information diffusion

Cyber insurance can effectively diffuse cyber security information when two conditions are met. First, insurers need to have more and better information about risks than the individual insured. Insurers obtain information about these risks by insuring a large number of similar cyber risks. They can extract all kinds of information from the insured,

---

[436] Buhlmann and Jewell (1979), pp. 243-262.
[437] See Chapter 7, Section 7.3 for a description of risk pools in other sectors.

for example the accident probability, the size of the losses, the possible care measures et cetera.[438] Insurers are able to do this when they have long time series available or at least are able to aggregate claim data.

Insurance companies also have incentives to independently do research about efficient cyber security investments for the benefit of their clients and their own loss ratio's. Insurers can benefit from economies of scale in acquiring information on cyber risks. Hence insurance companies are repeat players, and it is likely that their process of information aggregation yields better information about risks and the possibilities to reduce them than their clients, being one-shotters.[439]

Secondly, the insurer needs to be able to efficiently diffuse this information to the insured via the insurance contract. Insurers can tie premiums to the insured firm's care level, by requiring the insured to take specific care measures, such as ensuring up-to-date operating systems and regular security backups.[440] 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.[441]

Cyber pooling. Where with regards to cyber insurance it is mainly the insurer that has incentives to collect and diffuse information among its clients, within cyber pooling it is the individual organization itself that gains increased incentives to diffuse information. With regards to the

---

[438] Skogh (1991), pp. 360-370.
[439] Galanter (1974), pp. 95-160.
[440] Kesan et al. (2004); Biener, Eling and Wirfs (2015), pp. 131-158.
[441] Wagner (2009), p. 379.

other two risk allocation structures, the participant in the cyber pool has the strongest intrinsic incentive to diffuse information because the participant has a share in the risk of other participants in the pool.[442] Hence sharing information will directly benefit the individual that shares the information, when that information leads to risk reduction in the pool. Especially in homogeneous pools, the speed and relevance of information diffusion could be high.[443] This advantage strengthens when pools are homogeneous and individual organizations can make good estimations about the type of information needed by the other actors. Sometimes these organizations even have more information about efficient risk reduction than an insurer would have. This is particularly an asset to reduce the risk of information being out-dated in cyber security.[444] However, the scope of information diffusion is smaller in a cyber risk pool, because the information diffusion will be limited to the members of the pool and the number of members in a cyber pool is smaller than in an insurance pool because the members must be able to mutually monitor each other.

5.4.2 Internalizing externalities

Shifting risk can internalize the externality in cyber security.[445] The actor (or group of actors) exposed to cyber risk has incentives to manage it towards its own private optimum because he will bear the costs of cyber insecurity. The exposure to cyber security risk changes in the three risk allocation structures.[446] Hence, the structure of risk allocation determines the incentive organizations have in making

---

[442] Gordon, Loeb, Lucyshyn (2003); Anderson and Moore (2006).
[443] It should be noted that the first trade-off in risk pooling design emerges here. A homogeneous pool is good for information diffusion and mutual monitoring, while a heterogeneous pool is better from a risk spreading perspective.
[444] See Chapter 1, Section 1.5.2.
[445] See Chapter 1, Section 1.5.1.
[446] Zhao, Xue and Whinston (2013), pp. 123-152.

socially desirable investment decisions. A cyber insurance company has market-based incentives to increase the level of cyber security of the insured. This increase in the level of care increases social welfare if the costs of investments are lower than their societal benefits. Insurers have an advantage of taking into account social effects because an insurance pool - at least partly - will internalize externalities associated with cyber security.

Because the participants in a cyber risk pool have an equity stake in each other's risk, positive and negative externalities from information security investments can be partly internalized. Insofar as those externalities do not extend beyond the pool members, they will be fully internalized.[447] Hence, a cyber risk pool will also internalize externalities, but on a smaller scale, because the number of participants in the pool will usually be lower than with regards to cyber insurance.

In case of individual risk management there is no risk shifting and no risk sharing whatsoever. In other words, individual risk management does not solve any risk aversion since it is only the operator who remains exposed to the risk. Hence, individual risk management - ceteris paribus - does not contribute to the stimulation of information diffusion and the internalization of externalities.

5.5. The Storyline of Chapter 6 and 7

It becomes clear that the status quo, the individual management of cyber risk, does not produce sufficient incentives for contributing to the core overarching goal of this study, which is the stimulation of information diffusion in cyber security. The previous section has demonstrated that risk-shifting techniques are indeed capable of

---

[447] Gordon, Loeb and Lucyshyn (2003), pp. 461-485. This is also the case in insurance, provided that insurers can distinguish these externalities.

contributing to information diffusion (and the internalization of externalities). Assuming that organizations have a demand for shifting cyber risks, the question arises whether the particular features of cyber risks enable the two alternatives of risk shifting.

Chapter 6 will start with cyber insurance. I will empirically analyse the cyber insurance market for SMEs. This chapter will show that the very information deficits insurance could solve endanger the possibilities of risk shifting via the traditional instrument of insurance in the first place.[448] A general problem, which often emerges in insurance for relatively new risks, is that insurance companies may lack adequate information to be able to correctly calculate so-called actuarially fair premiums. This is a particular problem for cyber risks.[449] The insurers may suffer from insurer ambiguity and as a result charge a relatively high risk premium. If the potentially insured firm perceives this risk premium as excessive, demand and supply will not meet. That is the situation where a risk is considered uninsurable. It is more likely with newly emerging risks that this danger could occur. The problem arises that for new risks insurers often lack information and will therefore prudently charge (relatively high) risk premiums that may be considered as excessive by the individual firm. As a result insurance for newly emerging risks is often difficult.[450] Thus, cyber insurance could in theory enable risk shifting, provided there is sufficient information to calculate risks. However, Chapter 6 will show that the market (for SMEs) has not fully developed yet, precisely because of the lack of past data, subsequent high premiums, hard to unravel policies

[448] Externalities and information deficits are extensively discussed in Chapter 1, Section 1.5 of the study.
[449] See section Chapter 1, Section 1.5.2.
[450] Faure and Hartlief (2003), pp. 85-87.

and insufficient awareness among the public. The present cyber insurance market also seems to struggle with a particular feature of cyber security risks, which equally endangers insurability: correlated risks and cascade effects caused by the interconnectedness of IT-systems.[451] I will conclude that cyber insurance does not offer perfect incentives for managing the capricious cyber risks.

It is precisely for lacking information with insurers concerning (cyber) risks that risk sharing between organizations may be relatively attractive.[452] In some cases operators themselves may have better information on the relative nature of the risk than insurers. Chapter 7 will formulate conditions for cyber risk pooling. Provided that these conditions are met, I argue that cyber risk pooling can potentially move organizations to desirable (hybrid) forms of risk allocation where also individual management and cyber insurance play a role. Cyber risk pooling, so I will argue, can potentially provide ex post compensation to risk averse operators to cover damage caused by cyber risks; at the same time it can contribute to the *ex ante* prevention of cyber risks, thus increasing cyber security in society. In that sense cyber risk pooling can generate positive externalities for society at large.

[451] Biener, Eling and Wirfs (2015), pp. 131-158; Nieuwesteeg, Visscher and De Waard (2016); ENISA (2012).
[452] Skogh and Wu (2005), pp. 35-51.

6. CYBER INSURANCE CONTRACTS: A CASE STUDY

6.1. Introduction[453]

This chapter studies the opportunities and challenges of the cyber insurance market.[454] The focus is on SMEs and the Netherlands. I will empirically analyse to what extent current cyber insurance contracts for SMEs contribute to social welfare, and what options exist to improve these contracts to utilize the potential of cyber insurance. This chapter directly contributes to a stream of cyber insurance literature that mostly concerns case studies in the United States from the early 2000s.[455] While more contemporary studies on cyber insurance broadly discussed the insurability and description of cyber risk, they mostly

---

[453] This chapter is based on three publications. The first in the context of the LDE Centre for Safety and Security: Nieuwesteeg, Visscher & de Waard (2016) (<http://www.safety-and-security.nl/uploads/cfsas/attachments/The%20Law%20%26%20Economics%20of%20Cyber%20Insurance%20Contracts%20-%20A%20Case%20Study.pdf> (accessed 30 March 2018)). The second is a publication in the Dutch journal 'Het Verzekerings-Archief', also by Nieuwesteeg, Visscher & de Waard (2017). The third is a publication in the international journal 'European Review of Private Law', also by Nieuwesteeg, Visscher & de Waard (2018). In phases, the text of this chapter can be identical to the text used in these publications. In the pursuit of these joint publications, I made an independent and definable contribution. However, views and errors remain my sole responsibility.

[454] For insurance in general, see Ehrlich and Becker (1972), pp. 623-648. For cyber insurance, see Hofmann and Ramaj (2011), pp. 312-323; ENISA (2012); Biener, Eling and Wirfs (2015).

[455] Luzwick (1999), pp. 16-17; Jerry and Mekel (2001), pp. 7-36; Kesan, Ruperto and Yurcik (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 Van de Laar (2013), pp. 49-52. Obviously, the information and communication technology landscape has changed considerably in the past decade driven by smartphones usage, Big Data, Internet of Things and the availability of more easy to use cybercrime tools. See an extensive discussion in Chapter 1, Section 1.3. Hence, results that concern the state and development of cyber insurance deserve an update.

did not take into account the actual analysis of the policies and premiums itself.[456] Therefore, this chapter will analyse to what extent insurers respond to the challenges of the insurability of cyber risk and to what extent the cyber insurance market is currently capable of capitalizing on the potential of stimulating information diffusion in cyber security as described in the previous chapter.[457]

The chapter will demonstrate that insurers use different approaches to respond to the specific challenges of cyber security. On the one hand, some of the behaviour of insurers is aimed at gaining market share and eventually market size. A bigger market results in more data about cyber security risk. This is the first step to diffuse information about cyber security. However, cyber insurers appear to refrain from actually diffusing information. For instance, they deploy very little 'moral hazard measures'.[458] These are requirements the insurer gives to the insured in order to decrease the likelihood of claims. This is unused potential, since moral hazard measures are a means to diffuse information.[459] I also observe that some elements within contracts are primarily aimed at reducing (private) risk for the insurer, thereby lowering the likelihood that a market will develop. All in all, insurance companies seem to be halting between two options, on the one hand 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, especially for SMEs.

---

[456] Böhme and Schwartz (2010); Rawlings (2015); ENISA (2012); Biener, Eling and Wirfs, (2011).
[457] Chapter 5, Section 5.4.1.
[458] An example of a moral hazard measure that I did observe in the insurance contracts is the requirement to make a back up every week.
[459] 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 chapter is structured as follows. I start from the discussion of Chapter 5 about the potential of transferring cyber risk to an insurer in stimulating information diffusion and internalizing externalities. Section 6.2 introduces the main barriers utilizing this potential and their likely reflection in contacts, prices and competition. This section distinguishes external barriers (systemic risk and information deficits) from internal barriers (strategic behaviour to exploit information advantages.) This leads to theoretical expectations that will be compared with the actual state of cyber insurance contracts. Section 6.3 describes the setup for the case study, the empirical analysis of cyber insurance contracts for SMEs in the Netherlands. Section 6.4 presents the results of the case study that collected information on behalf of six different SMEs on actual cyber insurance policies from nine insurers operating on the Dutch market in 2015.[460] I will analyse and compare the draft insurance contracts on various aspects such as deductibles, caps, coverage, moral hazard- and adverse selection clauses, and requesting procedures. Moreover, I will analyse prices and participants in the market. Section 6.5 draws conclusions from the empirical analysis and provides ideas about how cyber insurance policies may be improved to optimally stimulate information diffusion.

6.2. Impediments to the Insurability of Cyber Risk

Chapter 5 discussed the potential of insuring cyber risk in order to stimulate information diffusion and internalize externalities.

[460] I requested cyber insurance contracts from all insurers offering cyber insurance on the Dutch market in 2015, but not every insurer was able to provide a draft contract.

Unfortunately, there are barriers to the insurability of risk.[461] There are external barriers (environmental issues) and internal barriers (issues between the insurer and the insured). The first two sections discuss external barriers. Section 6.2.1 shows cyber insurance coverage in relation with correlated risk and cascade effects.[462] Section 6.2.2 will show how the information deficit hinders the development of cyber insurance markets, prices and competition. The last three sections discuss internal barriers, most notably parties that strategically exploit hidden information. Section 6.2.3 discusses the problem of adverse selection, which manifests when there is an information surplus at the side of the insured before signing the contract. Section 6.2.4 discusses reverse adverse selection, an information surplus at the side of the insurer may result in strategic behaviour of the insurer. [463] Section 6.2.5 discusses moral hazard.[464]

6.2.1 The coverage of systemic cyber risk

Chapter 1 introduced the systemic character of cyber risk. This chapter discussed that the systemic element is caused by the high degree of interdependence between computer systems. Existing information

---

[461] See for a general discussion about the limits to the insurability of risks: Baruch Berliner (1982), p.13; Faure and Hartlief (2003); Wagner in Van Boom and Faure (2007), pp. 87-112; Wagner (2009). Both (insurance) law and economics literature as well as economics of cyber security literature distinguish several elements that hinder the insurability of risk.

[462] See Chapter 1, Section 1.3.5 for an introduction on systemic risk. The hampered insurability caused by correlated risk also occurs in other systemic risk. The literature on the law and economics of systemic risk provided useful insights and will be cited throughout through the chapter.

[463] 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 chapter will exclude reverse moral hazard from the discussion.

[464] See among many others, Arrow (1963), pp. 941-973; Akerlof (1970), p. 488; Shavell (1979), pp. 541-562; Shavell (2004).

technology is designed in a similar way and consequently vulnerable to the same incidents, hence incidents are potentially highly correlated between firms.[465] This section will discuss the impact of the systemic character of cyber risk on the development of cyber insurance and more specifically the coverage.

Risks in an insurance pool need to have some degree of independence from each other. However, the systemic cyber risk is not (fully) independent and has some degree of correlation. Consequently, the risk of an insurance pool does not equal average risk: the law of the large numbers does not work. After all, if a large fraction of total risk would materialize together, the insurer would not be able to provide coverage for all these simultaneous losses. Thus, correlated risk makes the insurance pool inherently less stable than uncorrelated risk. Closely connected to the fact that risk should be independent 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. Cyber 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.[466] It is difficult to observe to what extent and which cyber risk affects the continuity and solvency of an insurer. Still, general categorizations can be made, for instance, the distinction between correlated risk and cascade effects. Correlated risk in an insurance portfolio is risk that simultaneously affects several insured parties. Cascade effects occur when the operationalization of one risk as such causes a domino effect

[465] Baer and Parkinson (2007), doi:10.1109/MSP.2007.57 (accessed 30 March 2018).
[466] See for third party damage Kunreuther, Hogarth., and Meszaros (1993), pp. 71-87; see for second party damage Bandyopadhyay, Mookerjee and Rao (2004).

at third parties.[467] A matrix of these types of risk is displayed in Table 26.

Table 26: Correlated risk versus cascade effects from the perspective of the insurer

	Cascade effects (third parties are hit)	
Correlated risk (identical risk operationalizes at 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 and hence aggravated systemic uncertainties.

In case there are neither cascade effects, nor correlated risk, the risk is in theory independent, and hence insurable. There are for instance types of coverage that will only operationalize when first party risk is not correlated. An example is reputation damage or, to a lesser extent, the coverage for fines.[468] When only one company is hit by a cyber

[467] See also the discussion in Chapter 1, Section 1.3.5.
[468] The coverage of administrative fines in itself is disputable from a societal standpoint, because it could lead to moral hazard and a diminishing deterrent effect of the law.

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 this kind of third party risk are a simple option to mitigate uncorrelated third party risk, but caps have the social disadvantage that a part of the damage will not be covered by the insurer and hence the aversion of this uncovered risk at the insured is not remedied. With regard to risk that is indeed correlated, the systemic element increases significantly. In that case, as discussed before, risk, for example an exploit that allows for the installation of ransomware, can operationalize simultaneously among several insured in the pool. The law of the large numbers is not applicable anymore. When cascade effects occur together with correlated risk, total impact will be magnified.

What is the implication of the systemic element of cyber risk for the socially optimal design of cyber insurance coverage? The question is whether the category of cyber risk that SMEs want to insure overlaps with the category of cyber risk that insurers are willing to insure, given the aforementioned systemic uncertainties. Arguably, social welfare could be increased when SMEs can transfer cyber risk they cannot bear (i.e. low probability - high impact risk) 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 risk that they can bear (low impact risk). 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 SMEs 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.[469]

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. Many organizations possess large records of third party personal data. For these organizations, a high demand for insuring the potential costs related to third party damage can be expected. These costs include claims, fines, legal expenses, and crisis control expenses in case of loss of client and/or company information. On the other hand, for the insured, insured risk that has a high likelihood of being correlated might be difficult to insure because of its negative impact on the distribution of the insurance pool.

The paragraphs above illustrated the multitude of cyber insurance coverage design parameters. The question arises whether it would be desirable that insurance companies offer the same (basic) 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 deficits, which will be discussed in Section 6.2.2. On the other hand, fixed contracts do 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

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

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.[470] 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 risk.

Within cyber insurance, the extent to which an insurer accepts the transfer of risk depends on its own risk preference and on its ability to effectively mitigate and disentangle the correlation between various types of cyber risk. Insurers can take measures to reduce the correlated character of risk, by getting more customers and diversify among operating systems, sectors and countries.[471] So, which risk should a cyber insurer include, and which risk should a cyber insurer exclude? In a socially optimal situation, insurers solely exclude cyber risk that has a high likelihood of affecting their solvency and liquidity. It could be that, due to the lack of data, insurers could have wrong 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 include risk in their policies that they can bear. For instance, when insurers only have a few customers, how likely is it that correlated risk indeed affects their solvency ratio's, which justify low caps? It is important to note in this respect that this research focuses on the analysis of cyber insurance

---

[470] *Travelers Indemnity Co. of America* v. *Portal Healthcare Solutions LLC*, case number 14-1944, in the US 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.

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

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 insurer's 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 risk, with limited information about risk forecasts and the degree of correlation, one might expect that risk averse insurers would prefer the 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 risk, as well as exclusions for risk that is reasonably believed to be non-catastrophic or not extremely correlated, according to the aforementioned private optimum of the insurer.

6.2.2 Prices and competitors, the impact of information deficits

Information deficits are the cause of uncertainty about the future distribution of risk and loss potential, which are of importance in determining premiums.[472] Given the relative youth of cyber insurance, there is simply only limited actuarial historical data available.[473] Recall the information temporality discussed in Chapter 1, Section 1.5.2. Here it was illustrated that the cyber security landscape and risk can change

[472] Chapter 1, Section 1.5.2; Yurcik and Doss (2002).
[473] Ibid.

very rapidly. Consequently, actuarial data loses its value quickly to accurately forecast future risk distributions.[474] Information deficits (together with the systemic character) are widely acknowledged as the root cause for the initial slow development of the cyber insurance market.[475] This section discusses the prices and competitors in the US, EU and Dutch cyber insurance market.

In the US cyber insurance market, the annual gross premiums written are an estimated 1.3 billion USD and growing 10-25% yearly,[476] and 32% in 2014.[477] 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.[478] Estimates of the fraction of US firms that has purchased cyber insurance in 2013 vary between 6 and 19%.[479] There are huge differences between sectors, running from 1-2% of firms in the manufacturing and health sector to 20% in the financial sector.[480] 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 DBNLs as discussed in Chapter

---

[474] Tajalizadehkhoob et al. 2014.
[475] ENISA (2012); Biener et al. 2014; However, as of 2017, the cyber insurance market continues to develop faster.
[476] Betterley (2013) <http://betterley.com/samples/cpims13_nt.pdf> (accessed 30 March 2018).
[477] Beshar (2015) <http://www.hsgac.senate.gov/hearings/protecting-america-from-cyber-attacks-the-importance-of-information-sharing> (accessed 30 March 2018).
[478] Luzwick (1999); Kesan et al. (2004).
[479] Willis estimates that 6-10% of the US firms purchased cyber insurance whereas the Harvard Business Review reports that 19% has done so (Willis (2013) <http://blog.willis.com/downloads/cyber-disclosure-fortune-1000/> (accessed 30 March 2018);
Harvard Business Review (2012)
<http://www.ferma.eu/app/uploads/2013/01/Cyber-risks-report1.pdf> (accessed 30 March 2018).
[480] Willis (2013).

4.[481] Especially financial institutions regard cyber risk as a very important risk to deal with.[482] In 2013, approximately 10% of European firms was actually insured.[483] The annual gross premiums written equal 192 million USD in 2013 and are expected to reach 1.1 billion USD in 2018.[484] For the Netherlands, no accurate sales figures are available. The Dutch Association of Insurers concludes that cyber risk is by far not as insured as in the US,[485] even though, according to the association, cybercrime in the Netherlands is estimated to cause at least 13 billion USD in losses, possibly even two or three times as much.[486] However, there are also studies that stress that sometimes the cost of cybercrime is exaggerated.[487] '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.[488] 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. I co-designed a survey among

---

[481] ENISA (2012).
[482] Greenwald (2014), <http://www.businessinsurance.com/Article/20141023/NEWS07/141029882> (accessed 30 March 2018).
[483] Marsh (2013) <https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20Survey%2006-2013.pdf> (accessed 30 March 2018).
[484] NAIC (2013) <http://www.naic.org/cipr_topics/topic_cyber_risk.htm> (accessed 30 March 2018)
[485] Verbond van Verzekeraars (2013) <http://www.hiscox.nl/sites/www.hiscoxnl.com/files/filedepot/cyber-risks-informatie.pdf.pdf > (accessed 30 March 2018).
[486] Van de Laar (2013).
[487] Riek, Böhme, Ciere et al. (2016); The study labels this information incorrectness, as Chapter 1, Section 1.5.2. has illustrated.
[488] *Id*.

owners SMEs that did undergo an ethical hack.[489] 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 outweigh the benefits for SMEs. Also literature suggests that premiums are too high for SMEs.[490]

The question remains how insurers will respond pricewise to information deficits and what is a preferable reaction from a social welfare perspective. I 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'.[491] Insurer ambiguity follows the assumption that in situations where there is less insurability, insurers will increase the premium to incorporate the additional uncertainty.[492] 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 would likewise develop very slowly. Due to the lack of data, the fact that the pooling opportunities in a small market

---

[489] Dutch Network Group (2016) <http://www.dutchnetworkgroup.com/2878/grip-cybercrime-ondernemend-nederland.htm> (accessed 30 March 2018). I co-designed this survey together with the Dutch association for SMEs (MKB Nederland).

[490] Biener, Eling and Wirfs (2015).

[491] Kunreuther et al. (1993).

[492] Prices can also be high because of insufficient competition. Avraham (2012) mentions capital requirements, unfair competition or regulatory standards. *See* note 49.

are limited,[493] and the correlated risk in cyber security,[494] I expect that, in this scenario, only few insurers will offer cyber insurance.[495] 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 of the emerging new cyber insurance market 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.[496] 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 risk, they are often 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.[497] 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 risk, following from the discussion in Section 6.2.1.

---

[493] Yurcik and Doss (2002).
[494] Öğüt, Raghunathan and (2011), pp. 497-512.
[495] Van de Laar (2013).
[496] And taking relatively few adverse selection measures to increase the insurance pool even further.
[497] An 'MKB Meerkeuzepolis' of Achmea in 2015 with an insurable amount of 5 million euro. Details available upon request.

Hence, the second scenario is preferable from a social welfare perspective, because in such a situation welfare enhancing risk transfer and subsequently risk reduction measures can be taken. In such a situation I expect primarily large and diversified insurance companies entering the market, because they can afford to take potential losses when penetrating the market. All in all, 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 risk involved.[498] Insurer ambiguity therefore causes relatively high premiums and limited competition;[499] 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.

6.2.3 Adverse selection

For insurance in general, and for cyber insurance specifically, adverse selection is an impediment to market development.[500] Adverse selection results from the information advantage of the insured that he strategically can exploit before the contract is signed.[501] 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.[502] At least, there are high costs for

---

[498] Shackelford (2012); Betterley (2013).
[499] Biener, Eling and Wirfs (2015).
[500] Böhme and Schwartz (2010).
[501] For cyber risk 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.
[502] Akerlof (1970); Zweifel and Eisen (2003), p.59; Böhme and Schwartz (2010) assume this in their cyber insurance framework. Chapter 1, Section 1.5.2 also

the insurer in making the distinction between high risk and low risk insures.[503] Therefore (some) the characteristics of the insured, important for risk determination, remain undisclosed. This does not mean that an insurer cannot make a risk profile at all. Regarding cyber risk 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 sensitive personal data. But in most cases, an organization that wants to insure itself but has 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 risk 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, organizations 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 the pool.[504] An increase of average risk in the pool might force the insurer to increase premiums, after which firms with relatively low risk that were left might decide

---

discusses information asymmetries.
[503] Cooter and Ulen (2016), p. 48.
[504] Shackelford (2012).

to leave the pool, which increases the risk in the pool even further, et cetera.[505] 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.[506]

There are various contractual solutions that mitigate the effect of adverse selection in cyber insurance. I discuss the desirability of exclusion clauses, application forms and deductibles.[507] 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 sufficient data and accurately estimate risk distribution in the pool. The trade-off between reducing adverse selection and improving data is similar to the discussion in Section 6.2.1 on coverage and prices. The adverse selection measures aimed at aligning risk 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

---

[505] See the seminal contribution of Rothschild and Stiglitz (1976) in this respect and Chiappori and Salanié (2000).
[506] 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.
[507] This means this chapter leaves many other adverse selection measures out of the scope of the 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.

above average risk. Because of their simplicity and conventionality, I expect insurers to include exclusion clauses for general types of business, especially for organizations with a high risk profile such as online gambling and adult industry. A more sophisticated way of exclusion is to exclude certain types of behaviour. These are exclusions in case the insured does not fulfil 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.[508]

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

Nevertheless, 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 and thus allow for a certain amount of diversification within the pool. It is questionable how reliable and necessary very extensive application forms are, as one might argue that many SMEs do not have sufficient knowledge about their cyber risk

[508] ENISA (2012).

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 only ask 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 signalling function of the perception of risk attitude.[509] Section 6.2.1 suggested that high deductibles may be beneficial to 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 6.2.5 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.[510]

Again, the expectations about which adverse selection measures in the policies would lead to a private optimum for the insurance companies

---

[509] Avraham (2012).
[510] Priest (1987).

are two-fold, and depend on the 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 risk, and is eager to know a lot about potential clients through extensive cyber security audits before the contract is written.[511] Here an auditing agency performs an extensive and costly inspection of the security behaviour 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, I 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.

6.2.4 Reverse adverse selection

Although there is little data available about the cyber insurance market,[512] insurers do have more information about incidents than

[511] Anderson and Moore (2008).
[512] ENISA (2012).

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 behaviour 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 would need.[513] When there is an information surplus at the side of the insurers and it is costly for potential insured firms to acquire this information, insurers can use this advantage to reduce adverse selection. Eventually, insurance companies could use their information surplus to adversely select their customers,[514] 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.

Although the previous scenario might lead to a private optimum for insurance companies, reverse adverse selection should be avoided to reach a social optimum. Transparency in the applicability and limits of the insurance contracts is the key concept in counteracting reverse adverse selection.[515] In doing so, relatively uninformed firms looking for cyber insurance are 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

[513] Riek et al. (2016).
[514] Avraham (2012) p. 32.
[515] Ibid.

unambiguous coverage boundaries.[516] Fixed contracts, with fixed coverage clauses, can aid in reducing reverse adverse selection. However, as is discussed in Section 6.2.1, tailor made contracts allow for more flexibility that might be needed given the fast changing nature of cyber risk.

6.2.5 Moral hazard

Moral hazard occurs after the insurance contract is closed.[517] The insured might start behaving differently (i.e. take less care) because he does not bear the losses of a damaging event himself anymore.[518] As Cooter and Ulen describe it: "Moral hazard arises when the behaviour of the insured person or entity changes after the purchase of insurance so that the probability of loss or the size of the loss increases."[519] It is too costly for the insurer to perfectly monitor the behaviour of the insured, which can therefore exhibit these hidden actions. This influences the expected losses, so that the insurance premium has to rise. Three types of moral hazard problems are relevant for the cyber insurance market.[520] First, the insured party can take fewer precautions against the insured risk, leading to ex-ante moral hazard. Secondly, the insured may take insufficient measures to mitigate potential losses in the event of an insured occurrence: ex-post moral hazard. Thirdly, an

---

[516] *Travelers Indemnity Co. of America* v. *Portal Healthcare Solutions LLC*, case number 14-1944, in the US 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 US District Court for the District of Utah.
[517] 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.
[518] See among many others, Arrow (1963); Pauly (1968); Rowell and Connelly (2012); Shavell (1979); Shavell (2004);
[519] Cooter and Ulen (2016), p. 48
[520] Bailey (2014), pp. 1-44.

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.[521] In case insurers are not able to distinguish between insured organizations that take proper care measures and organizations that do not, insurers charge higher premiums to all insured firms,[522] 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 utility gains are realized by the fact that insurers can transfer information about cyber security to the insured. The insurer may require the insured to take specific care measures, and decline or lower pay-out in case the care measures are not implemented or not taken sufficiently. Another socially desirable moral hazard measure is information sharing among insurance companies,[523] such as historical loss data, claim histories, and compliance audits. Due to information sharing, insurers are better able to tie individual premiums to 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 diffusion 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

[521] Shetty, Schwartz, Felegyhazi et al. (2010), pp. 339-347.
[522] Avraham (2012).
[523] Bailey (2014).

adjustment and underwriting protocols, and increasingly affordable cyber insurance policies.[524]

I expect individual insurance companies to impose measures in their contracts to counteract moral hazard of the insured, including partial coverage, caps on payable sums, co-insurance and deductibles.[525] Moreover, insurance companies most likely require certain care measures from their clients, and that careless behaviour from the side of the insured will lead to (partial) exclusion from payment. In order to combat ex-post moral hazard, I expect insurance clauses that partially expose the insured party to risk,[526] via caps on payable sums and deductibles for the same reason. In order to mitigate ex-ante moral hazard, I expect that the insurer differentiates premiums based on the security practices of the insured party,[527] and based on feature and experienced risk rating methodologies.[528] Further fine-tuning of the premium could be reached via bonus/malus arrangements or no-claim discounts. Some subsets of cyber risk tend to be relatively independent of one's care level such as malware attacks.[529] Those types of cyber risk are less prone to moral hazard.

---

[524] 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.

[525] Shavell (1979); Shavell (2004); Wagner (2009).

[526] Faure and Hartlief (2003).

[527] Shetty et al. (2010).

[528] Bailey (2014).

[529] Tajalizadehkhoob et al. (2014).

6.3. Empirical Strategy

This case study selected cyber insurance contracts for SMEs to compare actual offers in the market to the theoretical framework. 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 MS through the 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 might be generalized to other countries in the EU and other highly developed digital economies, 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.[530] 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 risk.[531] Also, because of the interrelatedness of cyber security risk, improving the 'weakest links' potentially also benefits better protected large organizations, for instance when SMEs function as a back door to infiltrate larger organizations.

I requested cyber insurance contracts on behalf of six firms. Three organizations are currently operating in the Netherlands and three organizations are artificially constructed:[532]

---

[530] De Kok, Prince and Span (2015).

[531] PGI Cyber (2015) <http://www.pgitl.com/explore/article/smes-are-vulnerable-to-cyber-attacks> (accessed 30 March 2018);
Fino (2016) <http://economia.icaew.com/news/july-2016/smes-vulnerable-to-cyber-attacks-and-it-threats> (accessed on 30 March 2018).

[532] An extensive description of the organizations is available upon request.

- **Arbinn** is a small consultancy company for the energy- and 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 harbour.

The firms vary in size and dependency on IT infrastructure, in order to analyse whether insurers differentiate their offers. Eigensteil and Desiderius are the only two firms with a turnover higher than €1,000,000. 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, I 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 my knowledge all insurance companies operating in this segment of the Dutch market were approached.

The overview of typical cyber insurance policies in Biener et al. (2015) is the starting point for the analysis of coverage clauses.[533] 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

[533] Biener, Eling and Wirfs (2015).

profit and legal liabilities). In addition, I 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.

6.4. Results and Discussion

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 discussed, followed by the price of the product and subsequently coverage, caps and deductibles and risk reduction measures. The discussion is ended with a more high level synthesis of insurers and their strategies.

6.4.1 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,[534] 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 four months to get an overview of the available offers in the market.

---

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

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 I 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, I observe two elements. First, I 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 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.

6.4.2 Premiums

The results show that premiums for firms with a turnover below 1 million are 0.26-0.53% of the insured amounts. For organizations 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 27 presents an overview. Figure 11 in Section 6.4.4 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 organizations for €250,000 coverage is €1,000, which does not seem insurmountable. Still, as an illustration, premiums for liability insurance for small organizations are much lower, e.g. €150.04 per year, with a coverage of €2,000,000.[535] 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. The off the record information exists in the fact that I asked insurers for the loss ratio and received indications of a loss ratio of 10%, which might indicate that the premium is indeed too high as compared to the exposures to loss.

Table 27: 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 I 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*	

None of the contracts contained a bonus/malus system in which no-claim behaviour is rewarded with lower premiums and vice versa. The

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

small differences between premiums offered for different turnovers also indicate that insurers are not interested in behaviour-based premium differentiation or that they simply do not have the right data and tools to do in a cost efficient way.

6.4.3 Coverage

We scored the various policies according to the framework of elements in 'typical cyber insurance policies' designed by Biener et al.[536] 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 at the time interval of performing the empirical analysis. The first three columns of Table 28 present a brief description of the insurable elements. The last column indicates how many insurers out of seven provide coverage for each type.[537]

Table 28: 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	Cost resulting from reinstatement	5

[536] Biener, Eling and Wirfs (2015).
[537] The detailed comparison is displayed in Appendix B at the end of this chapter.

	third's systems / disturbance of authorised access by clients / misappropriation of intellectual property	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

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.[538] These distinctions might be explained by the insurer's desire to discourage careless behaviour 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.[539] 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

---

[538] Chapter 1, Section 1.3.4 discussed the distinction between first party and third party damage. The distinction is especially relevant for SMEs, which have relatively limited assets but may cause substantial third party damage.
[539] The detailed comparison is displayed in Appendix B at the end of the chapter.

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, 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, explains legal terms in its own way, and list many exceptions for coverage. 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 organizations looking for insurance, but also for experts. I requested experts to group insurable losses in the order of importance, and they responded that they found it too difficult to rank them.[540] This lack of uniformity complicates making a well-considered choice for a specific cyber insurance product, especially for relatively uninformed SMEs. This difficulty for prospect insured to

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

assess and compare policies, might indicate that reverse adverse selection is present. Another explanation might be that due to the complex nature of cyber risk, the insurers want to precisely define their coverage, also demanded by recent case law in the United States, as discussed in Section 6.2.4.

Do insurers cover risk that has a likelihood of affecting their liquidity and solvency? Every insurer covers at least some risk that is 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 risk. There are very few types of coverage that actually cancel out the likelihood that other parties would be affected simultaneously. This means that insurers are willing to take 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 exposes them potentially to vulnerabilities in cloud platforms. Apart from that, all insurers cover risk that is typically uncorrelated, such as reputation damage. Some insurers also cover administrative fines. As section 6.4.4 discusses, insurers impose caps on payable sums, which is also considered a means to reduce the risk on insolvency flowing from catastrophic cyber incidents.

6.4.4 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 organizations, caps vary between €250,000 and €1,000,000. For large organizations, there are observed

caps up to €2,500,000. Indeed insurers partially expose insured to risk via caps on payable amounts.

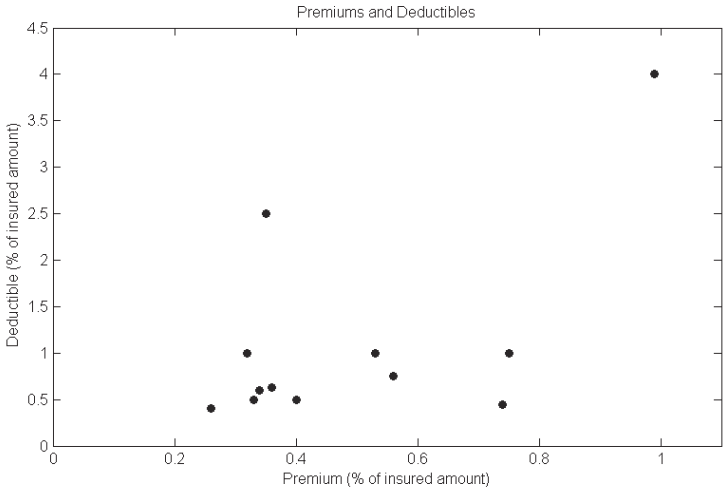


Figure 11: Premiums and deductibles

Figure 11 indicates that the deductibles vary between €1,000 and €100,000, or between 0.40% and 4.00% of the insured amount. It can hence be rewarding for organizations 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.

In the theoretical discussion in Section 6.2, it was 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 risk. However, on the contrary, the contracts observed contain relatively low caps and low deductibles. Relatively low caps can hinder demand for cyber insurance, because high impact risk is insufficiently insured. Moreover, relatively low caps, such as €250,000, could refrain organizations 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, at first sight attractive for buyers of cyber insurance, but not really necessary, since low impact risk is 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.

6.4.5 Risk reduction measures

Only AIG and ACE have 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 limited claim data hinders cyber insurers to make accurate risk reduction requirements for the insurance pool. Hence, most insurers solely use deductibles and caps as basic measures to reduce moral hazard.

6.4.6 Insurers and their strategies

I 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.[541] 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 and information diffusion. The discussion argues that there is currently a mixed view as to whether the market is capable of increasing social

[541] Verbond van Verzekeraars (2014).

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 focuses on offering products that mitigate its own risk 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.

I 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. I 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 reveal that. Anecdotal evidence from insurers themselves and the co-designed survey 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 'no-brainer' category such as the aforementioned prices for corporate liability insurance or property insurance.[542] 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 market for lemons (reversed adverse selection) exists in the sense that insurance contracts are mostly difficult to request. Moreover, prices and coverage are difficult to compare. It took us 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.[543] Hiscox covers administrative fines for non-compliance with DPL, while Chubb does not, and, vice versa, solely Chubb covers vicarious liability, when IT systems are outsourced. I 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

[542] 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.
[543] The detailed comparison is displayed in Appendix B at the end of the chapter.

compare coverage and pricing details and aggregate data in order to better forecast risk distributions. On the other hand, standard forms may also prevent competition and quick response to new developments in the market.[544]

A missed opportunity is the limited amount of risk reduction measures. As said, I only observed two insurers that set incentives for careful behaviour. 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 risk in two ways. On the one hand, I observed a more traditional insurer approach, where a lot of information is asked to 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, I 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.

6.5. Conclusions and Future Research on Cyber Insurance

6.5.1 Conclusions

Cyber insurance can potentially stimulate information diffusion in cyber security and social welfare. However, there are also barriers for growth of the cyber insurance market. What lessons can be learned from studying actual cyber insurance contracts for SMEs? Some elements in cyber insurance contracts foster growth such as the sometimes simple requesting procedure and the lower premiums than

[544] Avraham (2012).

several years ago. But I also identified several impediments to social welfare surplus. Insurers currently insufficiently focus their coverage on low impact high likelihood risk, possibly driven by a lack of information in the market. This chapter draws the inference that currently it is difficult for SME to make a well-informed choice due to the difficulty to assess and compare most policies. Future empirical research on behaviour of buyers of cyber insurance products should further scrutinize this. The information deficits on the side of the insured can be explained in two ways. Either it is a deliberate sustainment of a market for lemons, or it is the result of the fact that the development of the market is in an early stage which results in a variety of different types and of coverage. A last important sign is that information diffusion has not reached its optimal levels. For instance, only 2 out of 7 observed insurers require certain risk reduction measures (and hence diffuse certain information about efficient cyber security investments). All in all, the chapter concludes 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 risk that reduces the potential of cyber insurance. A possible explanation for these findings is that traditional insurers, which might not have adequate experience to insure cyber risk, offer cyber risk insurance. Cyber risk is a completely different category of risk and has a different lifecycle than other risk that those companies traditionally insure.

Naturally, given the rapidly changing nature of the Internet, the results are a snapshot and it is not unlikely that the premiums analysed in the case study will differ in the future. In addition, I 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.

6.5.2 Future research on cyber insurance

This analysis on cyber insurance contracts opens various avenues for future research This section briefly discusses some suggestion for future research.

Basic coverage. 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 risk. 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 organizations who have bought insurance to actually not be insured for such risk due to overlooked exclusion clauses. Additional insurance (either for other types of risk, 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 risk (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.

Mandatory disclosure of claim data. In order to tackle the problem of data unavailability, one could consider the social cost and benefits of 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.

Simplify requesting procedure. The requesting procedures for cyber insurance for SMEs are often very time-consuming and complicated. I 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.

Overlap with property insurance. Furthermore, it is worth investigating the overlap of cyber insurance with traditional property insurance. Many SMEs have the perception that cyber risk is already covered by traditional insurances.[545]

Alternatives for cyber insurance. Alternatives for cyber insurance should be thoroughly analysed. Common solutions to the issues of systemic risk are co-operation between insurance companies on data sharing, re-insurance, mandatory insurance, pooling and state intervention.[546] Several scholars have argued that pooling between organizations in particular can have advantages when the insurer has not more information about the market than the insured.[547] The next chapter will study the conditions for cyber risk pooling.

---

[545] Verbond van Verzekeraars (2014), <https://www.verzekeraars.nl/verzekeringsbranche/cijfers/Documents/VerzekerdVanCijfers/2014/Verzekerd%20van%20Cijfers%202014.pdf> (accessed 30 March 2018).
[546] Faure and Hartlief (2003).
[547] *Id.*

Appendix B

Appendix B.1: Coverage of third party liability per insurer

Table 29: Coverage of Third Party Liability per Insurer

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.

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	Consultants (legal, IT, forensic, PR) and notification/ monitoring costs	7	Y	Y	Y	Y	Y	Y

		relations expenses)								
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

Appendix B.2: Coverage of first party liability per insurer

Table 30: Coverage of first party liability per insurer

Coverage	Cause of cyber loss	Insured Losses	Comments on the interpretati	#	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 intellectu		4	Y	N	Y	Y	N	Y

		al property (e.g. software)								
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 paymen t	5	Y	O	Y	Y	Y	Y

Appendix B.3: Details of coverage of third party liability

Table 31: Details of Coverage of Third Party Liability for ACE, AIG/AON and Allianz

Coverage	Insured Losses	ACE	Notes	AIG/AO	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, deductible 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 32: 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 mention ed	Y	p.27: A system is interpreted as also including licenced systems.	N	Not mention ed
	Crisis control (e.g. cost of notifying stakeholder s, investigatio ns, forensic and public relations expenses)	Y	Paragrap h 1.6 and 1.7	Y	p.5	Y	p.3.
Network security liability	Cost resulting from reinstateme nt	Y	Paragrap h 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	Y	p.3.

					from the system of the insured (p. 20)] is not excluded p.7 (2.1) (d) (ii) Hence third party damage is covered.		
	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

Appendix B.4: Details of coverage of first party liability

Table 33: 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	Y	paragraph 4.1 p5	Y	When caused by insured or system failure: reasonable	Y	paragraph 1.7

	replacement of data				and necessary costs (1.2.4)		
	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 34: 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

7. CONDITIONS FOR CYBER RISK POOLING

7.1. Introduction[548]

This chapter continuous the endeavour of Part III of the study to identify whether and to what extent risk shifting can contribute to information diffusion in cyber security. This chapter studies the law and economics of cyber risk pooling arrangements: risk sharing without an insurer. The concept has had limited attention in cyber security literature. I aim to contribute to the literature by examining the theoretical potential of cyber risk pooling and by distinguishing the conditions for pooling in order to work in cyber security. In doing so, this chapter builds upon the theoretical foundations for risk shifting in cyber security formulated in Chapter 5 and the insights related to the struggling cyber insurance market discussed in Chapter 6. These chapters showed that neither individual risk management nor cyber insurance offer perfect incentives for managing capricious risks in cyber security. I will show that pooling, under some circumstances, may be more effective than cyber insurance. The main question for future research is whether risk pools in cyber security are capable of compartmentalization of risks and whether transaction costs of monitoring can be sufficiently low. I start this chapter by discussing cyber risk pooling in relation to the cyber insurance technique of the previous chapter in section 7.2. Section 7.3 addresses earlier experiences with risk pooling. This leads to the formulation of conditions for effective risk pooling in cyber security in section 7.4. Section 7.5 concretizes what ought to be specific design parameters of a pooling arrangement. I show which design choices should be made

---

[548] This chapter is based on an earlier publication: Faure and Nieuwesteeg (2018). In phases, the text of this chapter can be identical to the text used in this working paper. In the pursuit of this joint working paper, I made an independent and definable contribution. However, views and errors remain my sole responsibility.

in order to fulfil the conditions of an effective risk sharing agreement. I also distinguish the main trade-offs in such a design. Section 7.6 concludes.

7.2. Pooling Relative to Insurance

In this section, I will discuss pooling relative to cyber insurance technique, as discussed in the previous chapter. Theoretical studies mention various circumstances in which (cyber) risk pooling might be beneficial for participants and for society.[549] Borch was the first to analyse optimal risk sharing between two parties.[550] Arrow discussed various problems related to insurance, such as for instance the inherent problem of moral hazard.[551] It has especially been the Swedish economist Skogh who showed in a seminal article in the Journal of Institutional and Theoretical Economics (1999) that mutual and collective risk sharing between different agents can be beneficial when the probability distribution of losses is uncertain and hence impossible to estimate.[552] Skogh showed that mutually beneficial risk sharing is, differently than insurance, also possible without an assignment of probabilities. For insurance, the assignment of probabilities is always necessary in order to calculate a premium. In a risk sharing agreement partners can also share losses ex post. Risk sharing is possible as long as the partners in the pool are faced with the same risk. That also explains why an insurance market can only reach maturity when considerable actuarial information is available.[553] The alternative as

---

[549] Buhlmann and Jewell explore general forms of exchange that result in simultaneous improvement of risk for all parties (Buhlmann and Jewell (1979), pp. 243-262)
[550] Borch (1962).
[551] Arrow (1963).
[552] Skogh (1999), pp. 505-515.
[553] Skogh and Wu (2005), pp. 35-51.

such is thus not new, but to my knowledge, no practical application of sharing risks in cyber pooling has been applied so far.

7.2.1 Advantages

In this section, I describe the advantages of pooling relative to insurance. The main difference between insurance and risk sharing via pooling is that insurance always requires an assignment of probabilities in order to calculate a premium. Pooling, on the contrary, is more flexible to the unpredictable distribution of cyber risks.[554] Operators exposed to a similar risk can share risks even when the specific probabilities are unknown, while an identical unknown distribution of risks prevents independent insurers from using the law of large numbers that assumes that the actual pay-out on claims will converge to the average.[555] Skogh and Wu present the story of ship owners sharing losses to illustrate how risk sharing materializes.[556] The story is about the sharing of a potential loss of cargo and ship in a situation where no insurance is available. The two ship-owners have a similar ship, cargo, crew and route, and thus the same (unknown) probability of a loss. They would expect to benefit by sharing the loss of a ship. The two ship-owners also realised that the pooling would be more efficient if they would have more partners in the risk sharing group. But the offer to join the pool must be restricted to ship-owners

---

[554] Marshall identified two principles under which insurance might function: the reserve, or transfer, principle and the mutualisation principle. Under the reserve principle, risk is transferred to external risk bearers to hold in a reserve from which to discharge claims. With mutualisation, policyholders jointly hold the residual claims on the pool. Total losses are shared among policyholders by some combination of prepaid premium and retroactive dividend. The reserve principle is efficient when, by the law of large numbers, the average loss is predictable with virtual certainty while the mutualisation principle can be used in more general circumstances (Marshall (1974), pp. 476-492).

[555] Doherty and Dionne (1993), pp. 173-203.

[556] Skogh and Wu (2005), pp. 35-51.

with the same cargo and destination that could show a similar quality of ship and crew. A limitation in the pooling is the varying value of ship and cargo and varying destinations. But this shortcoming can be solved using a unit of measure, called a 'share', and then people can join the pool with different shares. In this way, the risks at sea are diversified. Since the pool members have a common interest in the prevention of accidents, they introduce safety regulations according to information available. As time goes by they also obtain further information on 'high' and 'low' risks. The tendency of low risks to leave the pool is mitigated by adjustments in the shares and the benefit of a large pool is therefore maintained.[557] For me, the tale gives a plausible picture of the development of pooling and the evolution of insurance. An additional point is that all citizens may beneficially share hazards that are unpredictable or not even foreseeable, as long as the presumption of equality is mutually accepted. The question remains whether such a presumption of equality can be established in cyber security risks.

Secondly, the pool has the flexibility to develop and issue specialized policies to its members. Risk pools have the flexibility to provide specific coverage or additional coverage beyond the scope of insurance companies.[558] Since participants are the 'owners' of a risk pool, the interest conflict between insurers and policyholders does not play a role in risk pooling agreements.

Thirdly, total costs can be lower. In an insurance policy, the risk is shifted to the insurer at the price of a premium. The premium is not recoverable by the insured no matter whether the insured risk

---

[557] Similar to a bonus/malus arrangements and no-claim discounts in the case of cyber insurance policies.
[558] Zhao, Xue and Whinston (2013), pp. 123-152.

materialized or not. In a risk sharing agreement, a member only contributes if an accident happens; the duty to contribute can either be postponed or the contribution can be carried over for the following year if there is no accident. A member can also recover his contribution by stopping creating the risk and leaving the pool. Another cost saving property of risk pooling is that expensive overhead and so called 'insurer ambiguity' costs are avoided.[559] The costs of ambiguity can be lower in a risk pooling arrangement when operators exposed to the same risk have better information on the risk than insurers.[560] In cyber security, this is especially the case when information is shared and aggregated.[561] Connected to the cost saving argument, a cyber pool might also be beneficial from a liquidity point of view, since money does not 'disappear' if nothing happens, it stays in the pockets of the participants of the pool.[562]

Fourthly, pooling can address the interest conflicts that arise between the insurer and insured. One of the most prominent interest conflicts is moral hazard that occurs after the insurance contract is closed.[563] The insured might start behaving differently (i.e. take less care) because he does not bear the losses of a damaging event himself anymore.[564] It is

---

[559] Ibid.

[560] Kunreuther, Hogarth and Meszaros (1993), pp. 71-87; on the other hand, when the insurer can effectively obtain the information from the insured, it can benefit from a potentially larger pool of insured relative to a risk pool and have a 'repeat player advantage', see Chapter 5, Section 5.4.1.

[561] Skopik, Settani and Friedler (2016).

[562] This depends on the funding structure of the pool, which I will discuss in Section 7.5.4.

[563] Moral hazard is closely linked to adverse selection, which occurs ex ante, before signing the contract in situation where complete information is absent. Moreover, it is often hard to distinguish moral hazard from adverse selection in empirical research.

[564] Shavell (1979), pp. 541-562.

too costly for the insurer to perfectly monitor the behaviour of the insured, which can therefore exhibit these hidden actions.[565] In a risk sharing agreement, mutuality is created, whereby the contribution paid by one member depends on the claims made by all other members.[566] It is in the interests of all other members' claims to be as low as possible and thus a mutual interest of risk minimization is created.[567] To reduce risks, the members of such a group have incentives to differentiate risks to align a member's contribution to the risk each member poses and to monitor each other. Mutuality is established when the members are subject to similar safety rules. The members are faced with the same type of risk and have often more expertise and precise knowledge compared to a third party insurer.[568] As far as cyber risks are concerned this may be the case, because they would have identical IT processes. Therefore they can evaluate the risk each member creates ex ante and can better monitor each other's behaviour.[569]

Because the likelihood that the members of the pool will have to pay depends on the performance of all members they will have strong incentives for mutual monitoring. If hence one member would free ride and not take safety efforts seriously this would create a moral hazard problem the same way as moral hazard arises in insurance contracts. Just as in insurance contracts monitoring by the insurer is indicated to

---

[565] Information asymmetry, such as between the insurer and insured, is an important property of cyber security risks. See also Biener, Eling and Wirfs (2015).
[566] Bennet (2001), pp. 13-21. Policyholders are themselves the owners of an insurance pool. Zhao, Xue and Whinston (2013), pp. 123-152.
[567] Bennet (2001), pp. 13-21.
[568] Faure and Fiore (2008), p. 302.
[569] Lee and Ligon (2001), pp. 175-190.

cure the moral hazard risk[570] in this case the pool members will have strong incentives for mutual monitoring in order to avoid that one risky member would increase the collective risk.

7.2.2 Drawbacks

First, an important condition for mutual risk sharing to work in its most simple form is that the parties in the pool must accept and trust that they all statistically face a similar risk.[571] Parties need to have a similar or at least comparable cyber security risk ex ante and need to carry out similar security efforts ex post. When this is not the case, the organizations that invest more will eventually drop out of the pool because for them the costs will exceed the benefits. In that sense, there is a danger that a risk pool may be unstable, because there will always be participants in a risk pool with a (slightly) better security position (ex ante or ex post) who will drop out, which may make the pool weaker. There is always the problem that pooling may be more attractive for participants that carry high risks. If these cannot be adequately identified, adverse selection will prevent pooling to emerge. However, even if risks are not homogeneous this not necessarily poses a problem as long as it is possible to differentiate and compartmentalize the risk and for example hold that the one who constitutes a larger risk pays a larger contribution to the pool.

Secondly, this danger of free riding will be worsened when mutual monitoring is impractical or impossible. In that case moral hazard may endanger the pool. As Shavell pointed out: "when monitoring is impractical, the optimal market response to moral hazard is generally

---

[570] Shavell (1979), pp. 541-562.
[571] Skogh (1998), pp. 247-264.

partial insurance coverage."[572] In cyber security, mutual monitoring can indeed be hard from a knowledge point of view but those who have the knowledge are fairly equipped to monitor participants in a pool.[573] This incentive for mutual monitoring will in principle be strong since the pool precisely has the incentive to control all of its members since the collective risk will increase if one of the members would free-ride. Precisely for technical and highly complicated (new) risks operators may in some cases have better information (compared to insurers) on optimal preventive technologies. That could be reflected in a differentiation of the contribution to the pool or in an exclusion of membership for bad risks. The question will of course arise to what extent the pool is indeed able to execute an effective mutual monitoring and thus to control moral hazard and adverse selection. If a differentiation between different types of risk would not be sufficiently possible, moral hazard cannot adequately be controlled and there is a likelihood that the pool will not emerge or that firms reduce their investment and free-ride on others.[574]

Thirdly, the setup of a pool requires an extraordinary effort and has large positive externalities, which are possibly too large to bear for one party. For the participant that sets up the pool it may be difficult to retrieve the costs it incurred in setting up the pool; he has to be either altruistic or to have a very large private benefit from creating the pool.[575] To overcome this situation in setting up a pooling arrangement,

---

[572] Shavell (1979).
[573] As indicated in an interview with mr. Rick Hofstede, cyber security analyst at Redsocks (21 Oktober 2016).
[574] Holstrom (1981).
[575] Of course, also one of the participants could initiate the pool and let other participants pay for the pool. However, setting up cyber risk pools is probably not the business of such a private initiator, which makes it extra costly (because there

a broker could be needed to set up a pool and guard the rules of the game. It that sense, the MSS, proposed by Zhao, can also be beneficial, because the private security party spreads knowledge and internalizes externalities.[576]

Another limitation of pooling is the fact that the capacity of the pool may be limited and that hence pooling cannot completely eliminate risk. This is a real problem in cyber security because, as indicated throughout the study, these cyber security risk can correlate, especially when organizations in a pool use similar IT systems which are vulnerable to similar cyber threats.[577] Unfortunately, this is quite often the case, since the IT products vendors are usually large players because of the economics of scale and lock in effects of the IT market.[578] In such a situation, a cyber risk pool may be worse than a cyber insurance pool, because the latter has more participants to absorb risk.[579] Additional insurance, beyond the cap that is set by the pool, might therefore be needed. Nevertheless, some cyber risks are less likely to correlate, as I will discuss in section 7.5.1.

Summarizing, there are three main potential drawbacks of pooling: the pool needs to be able to control the problems of adverse selection and moral hazard, there need to be sufficient incentives for creating the pool, and the pool needs to deal with the issue of limited capacity. Those drawbacks synthesize towards the formulation conditions for

---

is no experience) to start such a business. Precisely for that reason it are often large brokers that take the initiative to organize a risk sharing agreement.

[576] Zhao, Xue and Whinston (2013), pp. 123-152.

[577] I discuss the trade-off between risk spreading and mutual monitoring in Section 7.5.2.

[578] Varian and Shapiro (2004).

[579] When the cyber risk is not fully correlated between the participants of the insurance pool, otherwise the insurance pool is not a better instrument.

effective risk sharing. If these can be properly addressed cyber risk pooling may become possible.

7.3. Experiences in Other Sectors

There are certainly potential drawbacks of pooling and specific conditions that have to be met for pooling to work. Nevertheless, experiences in other sectors show that risk pooling can generate the benefits described in the literature. In addition to briefly describing the functioning of two existing pools (more particularly the functioning of the so-called 'Broodfonds' in the Netherlands and the 'P&I Clubs' that cover maritime risks) I will equally discuss two other initiatives where the creation of a risk sharing agreement proved more problematic. Enlightening the reasons why there were difficulties in the creation of those two other pools contributes to an empirical perspective on the formulation of conditions for successful cyber pooling.

7.3.1 Broodfondsen

A Broodfonds (literally: breadfund) is a risk pool in which self-employed people share their risks for incapacity for work.[580] The main reason why the Broodfondsen emerged in 2006 was because disability insurance for self-employed was expensive. In early 2016, there were 182 Broodfondsen that even backed each other financially in a form of re-insurance.[581] In an interview with the founder of the Broodfonds, it

---

[580] I consulted the following websites: Gijzel (2016) <https://www.nrc.nl/nieuws/2016/03/22/nrc-q-ziek-en-zelfstandig-dan-is-een-broodfonds-misschien-iets-voor-jou-a1493495> (accessed 30 March 2018, Dutch); ZZP Nederland (2016) <https://www.zzp-nederland.nl/actueel/nieuws/zzp-broodfonds-sterk-sociaal-idee> (Accessed 30 March 2018, Dutch).

[581] In Wikipedia, the Broodfonds system is described in more detail: "the systems of the broodfonds is as follows: "a Broodfonds pays out Members of a bread fund group who fall sick. They receive donations from the other members in their group, the total amounting to a net monthly income. The participants open

turned out that mutual monitoring functions well, since the self-employed "regularly meet and check upon each other".[582] The check-ups also have a social function, since participants also mutually share knowledge and ideas. All in all, the loss ratios and costs are much lower compared to forms of social insurance for unemployment. It is unclear whether this is created by self-selection or through actual better monitoring and early check-ups.

7.3.2 P&I clubs

Another example of a mutual risk sharing agreement comes from the maritime area and is provided by the so-called protection and indemnity clubs (P&I clubs). A P&I club is a non-profit making mutual insurance association which is established by ship owners and charterers to cover their third party liabilities related to the use and operation of ships. Today thirteen separate and independent clubs cooperate together to form the international group of P&I clubs, which accounts approximately for 90% of the world's ocean going tonnage.[583]

In the area of maritime transportation, the technical uncertainties with regards to the occurrences of oil spills combined with the legal uncertainties about establishing liability make it difficult to cover

---

individual bank accounts dedicated to their 'bread fund'. On these accounts the people who join a *broodfonds* save a fixed amount per month: between €33.75 and €112.50. They also pay a one-time service fee of €250 and a monthly contribution of €10. If members fall sick, they receive net donations depending on their own monthly contribution: between €750 and €2500. Personal donations can be tax-free under Dutch tax law. The monthly savings that accumulate on the bank account of each member are considered as personal savings and when people cancel their participation they collect this sum." <https://en.wikipedia.org/wiki/Broodfonds> (accessed 30 March 2018).

[582] Interview with Biba Schoenmaker, founder of Broodfonds (11 February 2016); see also <http://www.broodfonds.nl/hoe_het_werkt> (accessed 30 March 2018).

[583] See <http://www.igpandi.org/> (accessed 30 March 2018).

marine oil pollution via a traditional insurance policy. The P&I Clubs appeared as a response to commercial insurers' reluctance to underwrite marine risks.[584] P&I policies cover the liabilities specifically enumerated in the agreement - the Club's rulebook. P&I coverage usually includes "unlimited" reimbursement for claims arising from: liabilities in respect of persons, liability in respect of cargo, collision with ships, or with fixed and floating objects, salvage, compulsory wreck removal, fines imposed by government agencies, quarantine expenses, towage liabilities, "sue and labour" and legal costs, any other liabilities which the club's directors deem proper to cover as well as limited reimbursement for oil pollution claims which arise from the entered vessels.[585] The coverage of a P&I policy can be rather broad: not only does it provide a coverage to the liability for ecological damage, the relevant personal injury and property damage as well as other non-environment related losses are also covered. A P&I Club provides services more than a pure insurer and operates as a mixture of an insurance company, a law firm and a loss adjuster. Besides offering an insurance coverage, a P&I Club can also provide a worldwide network of correspondents and representatives to give on-the-spot assistance to the ship owner when required, give Letters of Undertaking to offer a security when members' vessels are arrested and assist in claims handling and settlement.[586]

---

[584] Ronneberg (1990), pp. 25-29.

[585] Ronneberg (1990), pp. 7-9. Ronnerberg's analysis was based on the Swedish Club's 1990 rulebook. A similar coverage can also be found in the 2010 rulebook of the United Kingdom Mutual Steam Ship Assurance Association (Bermuda) Limited. (Bermuda Rulebook) In the rulebooks, the "unlimited" reimbursement does not mean that the Club should pay the full costs which fall into the categories. Instead, the reimbursement is subject to the limitation of liability set by law. While for oil pollution claims, the compensable sums are determined by Directors of the Club.

[586] Ronneberg (1990), pp. 25-29.

Under the P&I policies, the insured must have suffered actual monetary losses before they can seek reimbursement from the insurers. That means a member is only entitled to seek compensation for the amount he has in fact lost due to the occurrence of a covered incident. This is called the 'pay to be paid' rule, which is usually incorporated in the Club's Rule Book. In a P&I policy, the Club is only obliged to assist his contractual counterpart, the Club's Member in case of losses. Thus usually, the injured cannot bring a direct action against a P&I Club and can only get the compensation by a claim, litigation against or settlement with the injurer.

The P&I Group arranges reinsurance together for each Clubs. At this moment, for the ship owners' policies, each Club retains the first $8 million as their retentions. The amount between $8 million and $60 million is divided among all the Clubs. The captive insurer of the Group - Hydra Insurance Company - and reinsurance with the international insurance market play an important role in providing reinsurance for the upper layers. This brings the upper limit of its reinsurance program to $3,060 million. Within this amount, the limit for compensation for oil pollution is limited to $1,060 million.[587]

7.3.3 Pooling offshore related risks

There are, however, also two examples that show that risk sharing can in some cases be problematic. One is the risk sharing in the area of offshore related risks. Two risk sharing agreements exist for offshore related risks, being OIL Insurance Ltd. (OIL) and OIL Casualty

[587] See also <http://www.igpandi.org/group-agreements> (accessed 30 March 2018).

Insurance Ltd. (OCIL).[588] Basically OIL and OCIL are risk sharing agreements between operators. They provide a maximum coverage of $300 million, but have a serious deductible of "not less than $10 million".[589] Notwithstanding the potential advantages of those risk pooling arrangements these risk pooling schemes are not very popular in practice. Major operators like BP are relatively critical of these risk sharing schemes in the offshore area. They argue that with those schemes risks are insufficiently differentiated.[590]

Moreover, operators also argue that the risk pools do not have a full solidarity since, depending upon the contractual arrangements, in some cases the liable operator will be compensated by OIL or OCIL but will have to repay (a part of) the damage over a specific (usually five years) period.[591] Also other major operators held that OIL and OCIL are not attractive for major players. The mutualisation in OIL and OCIL could lead to the danger for major players of smaller operators free riding on the majors in which case the majors would *de facto* become the guarantors of small players.[592] They argue that currently within these pools the risk differentiation is too low.

In this case, the problem is that damage can be potentially very high, but the probability is very low. Given relatively low probabilities of an accident the difference between a good risk and a large risk may be

---

[588] See Coccia (2012) <www.businessinsurance.com/article/20100912/NEWS/100919977> (accessed 30 March 2018).
[589] Faure, Liu and Wang (2015), pp. 389-390.
[590] Interview with representatives of BP (26 March 2013).
[591] Discussion with representatives of OGP (25 February 2013).
[592] Interview with representatives of Shell International BV in Rotterdam (14 March 2013).

that the good risks pays e.g. 30,000 dollars in contribution and a large risk 60,000. That difference is simply not large enough. The bad risk could simply pay a contribution and still free ride on good risks that have to contribute after an accident. Pools hence provide for smaller players with limited balance sheets some kind of safety net and risk differentiation is simply not sufficient.[593] In essence the problem of adverse selection cannot be cured as major players fear that they would have to back up for smaller players without sufficient risk differentiation.

7.3.4 Ria de Vigo

At a much smaller scale a risk sharing agreement was also attempted, but failed in the Ria de Vigo in North-West Spain.[594] A study showed that although a risk sharing agreement could be very beneficial for operators in the particular region, many misperceptions and objections inhibited the creation of a risk sharing agreement. Some operators confused risk sharing with a commercial, for-profit insurance; others did not understand that a risk sharing agreement would allow the transfer of risk and considered it more as a clearing house to transfer money. In the particular case of the Ria de Vigo the coming into being of a risk sharing agreement largely failed as a result of insufficient information concerning the benefits and working of a risk sharing agreement and the apprehensions about free-riders abusing the risk sharing agreement.[595] The latter example hence clearly shows the importance of a good communication towards the operators exposed to the risk concerning the potential benefits of a risk sharing agreement.

---

[593] Ibid.
[594] For details see Grossmann and Faure (2016), pp. 59-69.
[595] For details see Grossmann and Faure (2016), p. 68.

7.4. Conditions for Effective Cyber Risk Pooling

Section 7.2 discussed the benefits and drawbacks of pooling in comparison with cyber insurance. Risk sharing, so it appears also from the examples, can be an attractive tool to protect risk-averse actors in order to generate large amounts of compensation that can equally lead to better risk prevention via mutual monitoring. The same benefits can theoretically apply to the cyber security market as well. However, both the theory and the practical examples show that risk sharing may not under all circumstances be able to generate those benefits. Based on the literature and experiences from other sectors, three main conditions for effective risk sharing can be distinguished, which I will discuss in the three upcoming subsections.

7.4.1 Sufficiently unattractive alternatives

The first condition is that the alternatives for pooling, namely individual management or cyber insurance, must be sufficiently unattractive. In the case of P&I groups I observed pooling in situations where insurers did not want to enter the market while at the same time the harm of an individual incident could go beyond the solvency of an individual organization. Also, in the case of Broodfonds I observed that the insurance alternative was priced insufficiently competitive due to, among others, high information costs, while simultaneously the risk of being not able to work was too large to bear individually.[596] The fact that the alternatives are sufficiently unattractive is of course related to the theoretical advantages of risk shifting via pooling that I have sketched above (3.3). Especially for new risks like cyber security, insurance may suffer from high insurer ambiguity (with resulting relatively high risk premiums) and from the impossibility to calculate actuarially fair premiums.[597] Individual risk management may be

[596] Interview with Biba Schoenmaker, founder of Broodfonds (11 February 2016).
[597] Biener, Eling and Wirfs (2015).

relatively unattractive as it does not involve risk shifting and therefore neither provides ex post compensation, nor diffusion of information that could contribute to ex ante prevention. Cyber risk pooling can be relatively attractive compared to those alternatives as it allows pooling even when statistical probabilities of incidents are unknown (which is impossible with insurance) and since it can provide ex post compensation for damage, lower transaction costs and share information leading to ex ante prevention (which is impossible with individual risk management).

7.4.2 Effective mutual monitoring

A second condition is that the problems of adverse selection and moral hazard have to be controlled. Cyber risk pooling is obviously the easiest if all participants in the pool would statistically face a similar risk.[598] In that case problems of adverse selection would not arise. However, risk sharing of course does not require pure homogeneity. If for example two farmers would conclude a risk sharing agreement for the risk of their house being destroyed in a farm, risk sharing is still possible if for example one farm is double the value of the other one. That may simply imply that the farmer with the more expensive house has a larger share in the pool.[599] Also in the case of cyber risks the participants in the pool may not all constitute homogeneous risks. Pooling is still possible as long as the relative contribution of each participant in the pool can be appropriately distinguished and be related to his contribution. Also during the execution of the pool mutual monitoring is necessary to cure the problem of moral hazard.[600] In a cyber risk pool this can be done through the use network monitoring, where the participants of a pool or a third party

---

[598] Skogh (1998), pp. 247-264; see also the discussion in Section 7.4.2.
[599] See Skogh (2008), pp. 297-305.
[600] Skogh (1998), pp. 247-264.

continuously scan network traffic going in and out each participant. Network monitoring can be complemented by regular mutual audits related to the structure IT architecture and the up-to-dateness of software. The incentive for mutual monitoring will in principle be strong since the pool precisely has the incentive to control all of its members since the collective risk will increase if one of the members would free-ride. The different risks brought into the pool by various participants can be reflected in a differentiation of the contribution to the pool or in an exclusion of membership for bad risks. The question will of course arise to what extent the pool is indeed able to execute an effective mutual monitoring and thus to control moral hazard and adverse selection. If a differentiation between different types of risk would not be sufficiently possible, moral hazard cannot be adequately controlled and there is a likelihood that the pool will not emerge.

Mutual monitoring needs to take place without too high transaction costs. These transaction costs will be lower when risks are similar or at least comparable. In principle, since subjective probabilities do not need to be known ex ante[601] risk sharing does not require past loss experience or statistical information, which again can lower costs. The only ex ante information that is needed is the relative height of the risk of the participants in relation to each other. In a cyber risk pool a trade-off needs to be made to what extent one wants to monitor each other. With regards to network monitoring, there are fixed costs and economies of scale in the technical set up of a monitoring system. These costs logically lower when similar IT systems have to be monitored. However, the automatic detection of anomalies in a monitoring system's honey pot always leaves a residual that requires a manual

[601] Skogh (2008), pp. 297-305.

analysis with relatively high variable cost.[602] Last, mutual trust can lower these costs because it reduces the need for perfect mutual monitoring. It is the height of cost for mutual monitoring that largely determines the comparative advantage of cyber risk pooling to cyber risk insurance.

7.4.3 Practical possibility to set up a pool

A practical condition for effective risk sharing is that there must be a practical possibility to start in the first place. This means that there must be a party willing to take the initiative in setting up the pool. This requires not only that the potential participants are sufficiently aware of the cyber security risks to which they are exposed and that they must be aware of the benefits of pooling. But even if those conditions are met the difficulty may arise that it is simply costly and complicated to start a pool. Not only does it require a sufficient number of participants in order to have an adequate risk spreading; someone needs to take the initiative to start the pool. This could lead to substantial start-up costs. It therefore either requires one participant with a potentially large interest in starting a pool or a third party (in practice often a broker) who initiates the pool. In both cases the upfront costs for setting up the pool can of course be recovered from the participants. Besides, a degree of trust ex ante is most likely a catalyst for the start-up process. For example, when trust exists, participants are more likely to be tolerant towards the possible existence of slight inequalities in the size of the share of each participant in the pool.

7.5. The Design of a Cyber Risk Pool

Cyber pooling, so I showed, has advantages compared to individual cyber risk management and may be able to provide cover in cases

---

[602] Indicated by mr. Steffen Morrees, cyber security analyst at Fox IT (10 May 2017).

where cyber insurance may not. But risk sharing also has particular drawbacks and therefore conditions that have to be met before pooling can emerge. This section discusses the main design parameters for risk pool contract design in cyber security.

7.5.1 The covered risks

A risk pool is an alternative form of risk management. The first design parameter to discuss is thus, naturally, the choice of risks to include in a pooling arrangement. I discuss four perspectives for determining suitable cyber risks for pooling.

Impact. A first criterion is the impact of the risk.[603] The impact of the risk is of course directly related to the economic criterion of risk aversion. As I indicated above a demand for risk shifting will mostly emerge for relatively large risks, i.e. the risks of which the magnitude goes beyond the individual capacity of operators. Risks that have a small potential impact are easily manageable by individual organizations.[604] A demand for risk sharing via pooling will only emerge for risks that have a higher magnitude. Personal data breaches can result in significant costs, which consist of for instance legal sanctions, disclosure and mitigation costs and reputational damage.[605] However, a problem may equally arise with so-called catastrophic or high impact risks. High impact risks, especially those up to a level that is not bearable once distributed over the participants of the pool, are not suitable for pooling either, because the damage of an individual incident would go beyond the solvency of the participants in the pool.

---

[603] See also Chapter 1, Section 1.3.4.
[604] See Zhao, Xue and Whinston (2013), pp. 123-152. They argue that risk sharing (they call it RPA which stands for Risk Pooling Arrangement) is not effective if the risks are sufficiently small.
[605] Nieuwesteeg (2014).

The exact expected damage of cyber risks is often hard to determine.[606] However, as discussed in Section 7.2.1, pooling arrangements are more flexible towards unknown distributions. A widely used approach to determine ex ante which risks are included in a risk pooling arrangement is by setting caps and deductibles that basically set an impact interval where the pooling arrangement applies.[607] With the right cap and deductible, an ex ante determination of the potential impact of risks is not necessary anymore. Correlated risks remain as a residual, whereby multiple or even all the participants in a pool experience high impact at the same time. To mitigate the risk of correlated risks, the cap must be sufficiently low, or there must be a form of reinsurance in the case of strong correlation of risks.

Hybrid models. A pool that uses deductibles and caps is often part of a hybrid model where all three risks allocation structures (individual management, pooling, cyber insurance) are used. A cyber risk pool is almost always a part of multi-layered approach: Below the deductible, the participant individually manages its risk. This makes sense, because bearable risks should not be shared or transferred.[608] These are risks that are too small (minor data loss for instance) (or parts of bigger risks). Medium size risks are the risks suitable for pooling. The question is what are medium sized risks in cyber security, in terms of damage. An initial estimation could for example determine the interval of medium size risk between €500,000, and €5 million. On could think of severe DDoS attacks or significant loss of personal data. The maximum cap could be heightened through reinsurance, possibly

[606] Due to the nature of cyber risks discussed in Chapter 1, Section 1.3.
[607] A cap is a maximum amount for the pay-out. A deductible is an amount that must be paid by each participant in the pool before the common pool will pay.
[608] See my discussion in Chapter 5, Section 5.2 on the theoretical foundations of risk shifting.

between several risk pools.[609] For catastrophic cyber risks, risk sharing will not work as capacity to deal with these losses may simply lack in the pool. (Re)insurance can then capture the residual risk up to a certain level. Thus, (re)insurance is a possible solution, but in the current cyber insurance environment, both deductibles and caps appear to be relatively low.[610] This would then consist of a so called excess insurance where the insurance cover is only taken for damage above a certain level. In the previous example it would consist of damage above €5 million up to the limit of the insurable amount. Insurers use relatively low caps and low deductibles, while this type of product would require a high cap and (very) high deductibles.

Impact of care measures. It is important to study the effect of care measures on risk reduction. It is desirable to pool risks that are relatively independent from the care measures of the participants in the pool. In such a situation there will be less free riding and moral hazard because there is little or no relation between the activity level of the participant and the size of the risk. Hence, it is desirable when risks occur exogenously (i.e. cyber-attacks that are relatively independent from cyber investments of the participants in the pool). For instance, banking Trojans seem to occur relatively randomly at US banks.[611]

Systemic risks. Another important aspect is the correlation between the incidents of cyber risks. One major issue for both insurance as well as pooling is that cyber risk tends to correlate because they have systemic

---

[609] Brokers like Marsh and Willis provide these services, but only for very large companies. The Broodfonds organizes reinsurance with other Broodfonds pools.
[610] Nieuwesteeg, Visscher and De Waard (2016); See also Chapter 6.
[611] Tajalizadehkhoob et al. (2014).

character. Correlated risks, unfortunately present in cyber security at least on a theoretical level, hamper an efficient risk sharing. An option to mitigate the risk of correlation is to focus on those type of risks that have high internal but low cross-organizational correlation, such as insider attacks.[612]

7.5.2 Size and type of participants on the pool

In this section, I show the main trade-offs when choosing either smaller or larger groups, when selecting either homogeneous or heterogeneous groups (type of participants) and when choosing the organizational size of the participants.

Group size. I assume that the degree of internalization of societal risk increases if group size increases. Large groups are better capable of internalizing externalities because they form a larger part of society. Moreover, in order to create a sufficient degree of risk spreading, there needs to be a reasonable group size. The law of large numbers becomes more accurate when the group size increases. Consequently, larger groups will tend to approach the socially optimal behaviour better. An increased group size therefore better allows risk sharing.[613] However, with larger groups, the information costs also increase. This is caused by the fact that there are more transaction costs involved in mutual monitoring. Consequently, ceteris paribus, larger groups will experience more moral hazard and adverse selection. The impact of individual free riding on the personal risk distribution is also lower in larger groups, which decreases incentives to correct other participants. From a practical point of view, it is easier to set up a pool with a smaller group than with a larger group. Therefore, sufficient, but not too many

---

[612] Böhme & Kataria (2006).
[613] Lee and Ligon (2001), pp. 175-190.

firms should exist which ideally face a similar risk, as a result of which an effective diversification of risk would become possible.[614] In practice, I observed that effective risk pools have between 10 and 30 members. However, the exact optimum depends on, amongst others, the exact type of risk, the market and the expected damage.[615]

Type of participants. The type of participants is defined as the degree of homogeneity between the participants, in other words, the similarity in size of the organizations, IT processes, customers etc. Homogeneous organizations have fewer costs in monitoring each other in order to avoid adverse selection and moral hazard. For instance, if operators have the same software systems, then mutual monitoring is straightforward, but also the risk of correlation is higher and consequently risk spreading is lower. Further, homogeneity is a catalyst for knowledge diffusion, especially in cyber security. Consider a zero days hack at one of the participants in the pool.[616] A zero day threat is an undiscovered vulnerability that can be exploited by an attacker. Once the attack has been successfully executed, attackers will further utilize the zero day by executing attacks at similar organizations. Those vulnerable organizations are likely to include the other participants in a homogeneous pool. After a while, either a member of the pool or a third party such as the software vendor will discover the zero day. In such a situation effective knowledge sharing about the origins of the attack and solutions to fix it can greatly reduce overall damage in the pool. Note that here the speed of the knowledge diffusion is the main advantage. Moreover, setting up a risk pool is easier when organizations do not differ a lot in size and type, because

---

[614] Skogh (1998), p. 254.
[615] I observed this amount of members inter alia at the Dutch Broodfonds (Section 7.3.1). Also P&I groups usually have a size of this magnitude.
[616] As indicated by mr. Steffen Morrees, cyber security analyst at Fox IT (10 May 2017).

a base line defence effort can be observed more easily. Recall the difficulties in setting up a risk sharing scheme for the domain of offshore oil pollution: since there are large differences between the so-called major oil and gas producers on the one hand and smaller- and medium-size enterprises on the other, it is difficult to create a risk sharing agreement in which those largely diverging risk types can jointly participate.[617] As was mentioned above, differences in risk profile between the members of the pool are not necessarily a problem as long as this can be recognized and compartmentalized by the pool members. In that case principles of risk differentiation can be applied (by asking larger shares from the higher risk members). A differentiation of the contribution in that sense precisely constitutes an adequate remedy for moral hazard and provides incentives for prevention. On the negative side, there is more correlation between cyber risks when there is more homogeneity amongst participants in the pool, as it is likely that similar organizations use similar software systems and are vulnerable to similar kinds of attacks. Hence, there is a trade-off between *heterogeneity* and *homogeneity*. Heterogeneity allows for a better distribution of cyber risk, while homogeneity allows for better mutual monitoring, lower costs and faster knowledge diffusion.

Effects of participant size. As the example of risk sharing in the offshore oil pollution sector shows, the attitude towards risk (which is strongly related to the financial capacity of the operators) will strongly affect the demand for risk shifting and hence the willingness to participate in a pool. That problem will obviously also play in the case of sharing security risks. A demand for risk shifting can be expected to be higher with relatively small and middle-size operators than with larger operators. Larger operators may largely be able to cover risks

[617] See Section 7.3.

themselves and may hence have less demand for risk sharing. Moreover, larger operators may even fear that small- and medium-size operators would free ride on the mere size of the larger operators. That was the reason why it was difficult to create a risk sharing pool for oil pollution in the offshore sector and may to some extent equally play a role in case of cyber security. One way of potentially solving this is to create several risk pools with different types of players, each constituting relatively homogeneous groups. The obvious solution would then for example be to create one group for small- and medium-size operators and one for larger operators (to the extent that they have a demand for risk shifting at all). Separating those risks in different risk pools may, moreover, contribute to risk differentiation and thus better stimulate the preventive function of risk sharing.[618] A cyber risk pool that aims to deploy some kind of technical mutual monitoring solution arguably would need to consist of at least medium sized companies, because otherwise the costs of such a monitoring solution would outweigh the benefits.

7.5.3 Rules of entry

One of the key determinants of a successful risk pool is its ability to successfully monitor and select its participants *ex ante* in order to reduce adverse selection. An ex ante level of cyber security is also important to disentangle the impact of the risk from the care measures of the members of the pool, which is, as I argued in Section 7.5.1, preferable in order to reduce free-riding. If all members have an adequate ex ante level of security, attacks that take place can reasonably be believed to be not the result of careless behaviour.

---

[618] See Priest (1987), pp. 1521-1590. Priest strongly stresses the importance of segregating risks into relatively small risk pools with similar risks in order to prevent adverse selection.

Consider the example of ransomware. Ransomware is widely used by cybercriminals. However, an organization could greatly reduce the risk of ransomware by implementing the right (simple) care measures ex ante.[619] In the case of a cyber risk pool, it can be difficult or time consuming to determine the level of cyber security ex ante. A third party, such as a security firm, can objectively determine the level of security ex ante by performing a network assessment and issuing a certification. Often these certifications by private certifiers will be used as proof of compliance with particular security rules. One should however bear in mind that these certification processes are also subject to problems related to information asymmetry and moral hazard. Another option is to assume an ex ante security level and to set this level as a precondition for pay-out ex post. In a cyber risk pool, one could require an extensive logging that allows for tracing back the origins of the cyber attack and the organization's level of cyber security before the attack occurred. Moreover, government or private regulation can also assist in determining the required level of cyber security.[620] Apart from that, several design options are possible with regards to the decision making on the entry of new participants. In the situation of the Broodfonds, the members of the pool must agree unanimously to include a new participant in the pool. In this respect the administrator of the fund would play an important role. Often these are brokers or a 'managed security service'.

7.5.4 Contribution of each participant

One of the main advantages of the risk pool is the fact that the absolute height of the contribution of each participant does not have to be

---

[619] As indicated by mr. Steffen Morrees, cyber security analyst at Fox IT (10 May 2017).

[620] Although also here, there is a risk of governmental and/or regulatory failure, see Chapter 2, Section 2.3.1.

determined ex ante. However, it is still necessary to determine the relative share of each participant in the pool, which I will discuss in this subsection. The most standard form is that every participant has an equal stake. However, this gives an advantage to participants that are more likely to experience risk and can free-ride. In more complex situations where the risk of individual participants differs, (a mix of) other metrics can be used as proxy to determine the contribution, such as bandwidth, turnover and the average number of connected devices or data records. In such a situation, there is a risk that larger players do not want to participate in the pool because smaller players free-ride, especially when the difference between large and small is substantial. In order to have optimal incentives for prevention it may be clear that the contribution should in principle be risk-related. Good risks should therefore contribute less than bad risks. This risk differentiation, as reflected in the financial contribution, will provide incentives for prevention. The reverse would be the case in the absence of risk differentiation. That would happen if a flat fee contribution would be charged. Such a flat fee would invite free-riding as it would not provide any rewards for investing in additional safety measures. Most existing risk sharing agreements (like the already mentioned P&I Clubs) would therefore on the one hand impose minimum safety rules and on the other hand differentiate financial contributions according to risk. In order to provide adequate incentives for prevention the latter should also be the case for cyber security risks. Minimum ex ante safety rules could for instance be determined through the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27002 and the Centre for Internet Security (CIS) Critical Security Controls.

7.5.5 Timing of the contribution

There are various ways to fund a pool. Buhlmann and Jewell distinguish three types of risks pools.[621]

Paying ex ante. By paying a premium ex ante all participants pay a periodical fee The aforementioned members of Broodfonds pay a monthly premium to a separate bank account. The major advantage of asking a payment up front is that the willingness of all participants in the pool to contribute to the pool will be high ex ante when they do not know who will be victimized by the cyber security risk and they hence take a decision 'behind the veil of ignorance'. It avoids the problem that the members to whom the risk did not occur would ex post, with hindsight bias have a reduced willingness to contribute. The disadvantage of an ex ante payment is that it leads to an immobilization of capital.

Paying ex post. Paying ex post means that participants in the pool solely pool the risk, and they pay per claim ex post.[622] The advantage of this system is that members keep the optimal liquidity and there is no welfare loss caused by 'dead' money. However, uncertainty is increased since members cannot be sure that other members will pay. A possibility to avoid this uncertainty is to give a bank guarantee. Such a system exists with respect to a European system to cover pollution damage for offshore oil and gas installations, referred to as the Offshore Pollution Liability Agreement (OPOL). OPOL guarantees that specific funds will be made available to meet the claims since members of OPOL need to provide proof of financial responsibility. OPOL de facto provides mutual risk sharing as far as the insolvency of

---

[621] Buhlmann and Jewell (1979), pp. 243-262.
[622] Called a claims pool by Buhlmann and Jewell (1979), pp. 243-262.

one of the members is concerned. For that reason the solvency of the members is controlled since operators have different ways of showing financial responsibility.[623]

Hybrid payment. In the case of ex ante payment, the claims could exceed the accumulated funds. In such a situation a hybrid construction is also possible, a combination of prepaid premium and retroactive dividend.[624] In practice many existing risk sharing agreements use such a hybrid model. For example the P&I Clubs discussed above will in principle demand an upfront payment from their members. When a 'good' year occurred (without losses) the Club could decide not to ask a contribution for the next year. In case a 'bad' year happened (with relatively large incidents) an additional call on the members could be made.[625]

7.6. Concluding Remarks

In this Chapter I analysed the potential and conditions for using risk pooling as a tool to deal with cyber security risk. Risk pooling has often emerged as an alternative, mostly to insurance, especially for newly emerging risks. With newly emerging risks statistical information to allow an accurate pricing of the risk is often not available and insurer ambiguity may lead to high risk premiums as a result of which there may be no sufficient demand. The basic idea with risk pooling is that with particular risks operators may have better information on the risk exposure and the desirable measures to prevent the risk than insurers. When this is the case a pool can lead to mutual monitoring, thus stimulating information diffusion, a reduction of transaction costs and ex ante prevention of risks. I argued that if these conditions are present

---

[623] For details see Faure and Wang (2015), pp. 25-36.
[624] Marshall (1974).
[625] See Faure (2016), pp. 155-157.

risk pooling may create protection for individual operators who participate in the pool, but also positive externalities for society at large since the pool can contribute to the reduction of cyber security risks.

The main advantage of cyber risk pooling is that it can provide cover even when specific probabilities of an incident occurring remain hard to predict. Cyber risk is characterized by strong information deficiencies, such as information unavailability, temporality, asymmetry and incorrectness that hamper the objective determination of expected value for future cyber incidents.[626] Whereas insurance always requires the determination of a premium ex ante, pooling is possible without a pricing of the risk. It is necessary, however, to identify the relative contribution of the various participants to the pool. Based on these general starting points I examined the potential of risk pooling for cyber security. I argue that if sufficient information can be gathered by operators to differentiate the relative risk exposure and contribution of the various participants, the traditional problems of adverse selection and moral hazard (which can equally threaten the emergence of risk pooling) can be remedied. I also noticed that the major advantage of cyber risk pooling would not so much be compensation ex post (for which often insurance is used), but rather the information exchange that may be generated through the creation of a pool. It is the very necessity to reduce the lack of this information diffusion in cyber security that is one of the central notions of the study as Chapter 2, Section 2.2 illustrated.

Referring to other examples where risk pools were created, but also where risk pools failed, I pointed at the importance of a careful design of a cyber risk pool. To the best of my knowledge today cyber risk pooling has not yet emerged. However, I argue that there may be a

[626] See Chapter 1, Section 1.5.2.

large interest among operators to create those pools, not so much as tools for ex post compensation, but especially as tools for information exchange, leading to ex ante reduction of cyber security risks. The emergence of a risk pool, however, requires a correct understanding among operators of the cyber security risk and some degree of similarity (perhaps even homogeneity) in order to facilitate the risk pooling. It equally requires an active entrepreneur (like a broker) to initiate the pool. Moreover, risk pooling would never be the only instrument to deal with cyber security, neither as far as prevention, nor as far as compensation is concerned. With respect to compensation, a pool would probably include a large deductible as a result of which operators would still individually manage risks below the deductible. Such a deductible also reduces moral hazard. Moreover, pools usually include important limits; the very high (catastrophic) risks are often hedged to (re)insurers. It is therefore likely that in the future cyber risk pooling may take an important place in such a multi-layered compensation mechanism to deal with cyber security risk.

The goal of this chapter was merely to sketch that risk pooling could play an important role in cyber security and to show the specific conditions and design issues that would have to be taken into account in developing cyber risk pooling. Of course, the specific nature of the cyber security risk, as well as the different types of cyber risks, does deserve further detailed attention. It may potentially lead to the conclusion that various risk pools have to be created for specific types of cyber security risks. The way in which this can be designed in a more detailed manner as well as the interest of operators in participation in such a pool are issues that undoubtedly merit further research.

CONCLUSION

8. CONCLUSION AND SYNTHESIS

Over the last decade an increasing amount of cyber attacks threatened the functioning of the global economy. Estimations of societal damage easily surpass tens of billions of euros. The nature of cyber risk changes at an increasing rate and organizations must keep up. The 2017 Wannacry and NotPetya attacks are testament to the fact that organizations cannot permit to sit back and refrain from implementing - sometimes the most basic - security measures.

But, after a significant cyber attack, not a single day goes by without security companies claiming that the digital apocalypse is approaching. As much as doing nothing to protect oneself does not benefit society, neither does overinvestment in cyber security. It is very difficult for organizations to determine the right level of cyber security investment that will lead to an 'optimal' level of security. In order to attain optimal cyber security, this study advocates that information related to the nature of cyber risk and the return on investment of measures to reduce it needs to be shared among relevant actors, while taking into consideration the costs of doing so. Currently, there is insufficient information diffusion in cyber security, despite efforts such as ISACs, NCSCs, Chief Information Security Officer (CISO) talking shops and other venues for cooperation and knowledge sharing.[627]

This problem is caused by the strong public good characteristics of information diffusion; the party that diffuses information receives little benefit from doing so. Information deficits, externalities and market

[627] Especially for SMEs, see Chapter 2, Section 2.2.4. The study mostly focuses on diffusing information between organizations.

power hinder the spontaneous diffusion of information even further. Hence, this study seeks to identify solutions for efficient stimulation of cyber security information diffusion between organizations for university, government and industry, as its research question reflects:

> *How can university, government and industry efficiently stimulate cyber security information diffusion?*

In answering this research question, the analysis considers the factors listed below. These key factors are the building blocks of the study's storyline and together lead to the formulation of this study's three core ambitions. This final chapter reaches back to these ambitions, synthesizes the findings and provides concluding remarks.

Optimal security. What should be the goal of investing in cyber security? Rather than focussing on perfect security, the study advocates reviewing the cyber security theatre through the lens of optimal security. The goal of this utilitarian approach is to maximize social welfare, through an efficient level of cyber security investments. This level is reached when the marginal social costs of cyber security investments equal the marginal social benefits of reduced cyber insecurity. Consequently, organizations need to have sufficient information related to the nature of cyber risk and the return on investment of measures to reduce it.

The systemic cyber risk complicates the determination of this desirable efficient cyber security investment strategy. Cyber risk is correlated and an incident can potentially cause cascade effects at other parties. In cyber security, attackers have a systemic advantage over defenders. Also, the nature of these attacks changes rapidly. In this systemic cyber risk environment resilience is key, which means a focus on the risk of

failure after an attack occurs, instead of focussing on the risk of the attack occurring.

Market failures - externalities, market power and an information deficit – aggravate the problems of efficiently investing in cyber security even further. Market failures lead to underinvestment in cyber security relative to the socially efficient level. Of all the market failures present in cyber security, the study focuses on reducing the information deficit. Within the information deficit, the study distinguishes information unavailability, incorrectness, asymmetry and temporality.[628] The information deficit is one of the most tenacious market failures and solving it can potentially also reduce other market failures such as externalities and market power. However, in the endeavour of solving the information deficit issue, one will be inherently be confronted with these other market failures to begin with.

Information diffusion. A crucial approach to contribute to the reduction of the information deficit is the stimulation of information diffusion; the continuous circulation of cyber security information among relevant actors. Information diffusion has several benefits. First, increased information diffusion leads to increased efficiency in cyber security investments, because organizations can utilize information from other organizations and do not have to 'reinvent the wheel'.[629] Secondly, increased diffusion of data leads to better products, such as cyber insurance. Thirdly, information diffusion balances market power

---

[628] See Chapter 1, Section 1.5.2.

[629] As long as the costs of information diffusion are not higher than the benefits of not reinventing the wheel. Information diffusion realigns incentives and corrects market failures. See also Chapter 2.

of big software and security firms, as they will have fewer possibilities for exploiting information asymmetries. Fourthly, when information diffusion reduces transaction costs, this could lead to a reduction of the externality problem.[630] Unfortunately, there will be suboptimal spontaneous diffusion of information in the absence of additional incentives. Information diffusion has strong public good characteristics, which means that the actor that diffuses the information will not or limitedly benefit from it.

The triple helix. The factors above - the systemic cyber risk, market failures and the lack of spontaneous information diffusion - characterise the complexity of the cyber security theatre. Ergo, all societal forces must be mobilized to increase information diffusion. The three societal forces in the cyber security theatre are joined in the so-called 'university-government-industry triple helix'.[631] They each have different roles, responsibilities and tools. The deployment of the respective tools of these three parties (combined with their mutual cooperation) will yield the most fruitful results. The three substantive parts of the study all focus on the role of one party in stimulating information diffusion, although it should be noted that quite naturally

---

[630] Coase (1960).

[631] "The concept of the Triple Helix of university-industry-government relationships initiated in the 1990s by Etzkowitz (1993) and Etzkowitz and Leydesdorff (1995), encompassing elements of precursor works by Lowe (1982) and Sábato and Mackenzi (1982), interprets the shift from a dominating industry-government dyad in the Industrial Society to a growing triadic relationship between university-industry-government in the Knowledge Society." From Stanford (2017) <https://triplehelix.stanford.edu/3helix_concept> (accessed 30 March 2018). See also Etzkowitz and Leydesdorff (2000).

also the government and industry parties are analysed through the lenses of the university party.

Legal instruments. Two legal instruments, being regulation and contract, play a key role in all three parts of the study, as they provide the necessary additional incentives for information diffusion. In Part I, on the role of university in stimulating information diffusion, I have diffused information *about* a legal instrument. This part described a project in which DPL in cyber security was coded and unlocked for further comparative and statistical analysis. Hence, I performed the information diffusion myself, as an example of the potential contribution of this societal actor (since I am part of the university helix). Part II and III have a different point of reference. Here, I analysed the (potential) means government and industry may employ to stimulate information diffusion, namely the DBNL and two types of risk shifting agreements (cyber risk insurance and cyber risk pooling). Part II and III scrutinized whether those legal instruments, when performed by government and industry respectively, are capable of incentivizing organizations to engage in diffusing information. The substantive analyses of the three parts realize the first ambition of the study.

> **Ambition 1:** Contributing to the literature on data protection laws (Part I), data breach notification laws (Part II) and risk shifting agreements (Part III).

Section 8.1 will give a concise summary of Part I, II and III. In doing so, I will demonstrate to what extent these parts contributed to the specific literature as expressed in the first ambition of the study. Also, I will illuminate avenues for future research within these specific fields. The study provides examples of how the different tools of the three

different parts of society can be utilized. Nonetheless, the studies' deep dives show that the specific tools of university, government and industry can be deployed much broader. The study arrives at the discussion regarding this broader deployment when fulfilling in its second ambition.

> **Ambition 2:** Proposing an agenda concerning the stimulation of information diffusion in cyber security for the university, government and industry triple helix.

Section 8.2 formulates this agenda for the stimulation of information diffusion in cyber security based on the roles and responsibilities of university, government and industry. A necessary condition - or even necessary foundation - for reaching the first two ambitions is the proper application of law and economics to the field of cyber security. This has the consequence that the field of *law and economics* must be linked to the field of *economics of cyber security*. There are strong opportunities for mutual learning between these two fields. Scholars of the economics of cyber security can learn from the application of law and economics analysis to cyber security, such as the literature on optimal enforcement and risk shifting agreements. Scholars in law and economics can also benefit from insights from the economics of cyber security. This includes the core dynamics of investing in cyber security, such as threats, vulnerability, impact and strategies to reduce these. The economics of cyber security also provides insight into the specific microeconomic peculiarities of the systemic cyber security risk, such as far reaching externalities, various types of stubborn information deficits and persistent market power of security and software companies.

Currently, the fields are hardly linked at all. Chapter 1 revealed that mutual referencing to both disciplines is limited to on average 3-4% of total references. This is a low number, because within each discipline, only those subjects already largely overlapping with the other discipline are discussed (hence, either legal or cyber security). Without a doubt, the intersection of law and economics and economics of cyber security is fertile ground for contributing to optimal cyber security. When legal instruments are entering the cyber security theatre, scholars of law and economics and the economics of cyber security should work together in order to make sure they contribute to social welfare or at least show what the social welfare implications of these choices are. Within the context of the storyline of the study, the law and economics of cyber security should design and analyse legal instruments that contribute to information diffusion. Therefore, the third ambition of the study is to foster the further linkage between law and economics and the economics of cyber security.

> **Ambition 3:** Connecting law and economics with the economics of cyber security.

Section 8.3 discusses the necessity of and barriers to connecting law and economics with the economics of cyber security. I will give recommendations that will further develop this proposed *law and economics* of *cyber security*. Finally, I will end this chapter and study in section 8.4 with a few closing remarks.

8.1. The Three Parts of the Study

This section will provide a concise summary of the study. The three substantive parts treated four deep-dives in the law and economics of

cyber security. In doing so, I will also illuminate avenues for future research.

8.1.1 Part I

Part I embodied the role of university in stimulating information diffusion in cyber security. The unique ability of university is that it can apply scientific methodologies in full independence. The academic approach allows for building metrics about legal instruments that will eventually result in longitudinal data on the development of legislation.[632] These metrics foster the independent and academic scrutiny of the impact of legal instruments. Hence, Chapter 3 in Part I diffused information *about* the law. I used the law and economics methodology of QTA to compare 71 national DPLs that were applicable in 2014. Data protection is one of the most important and widespread legal instruments in the governance of cyber security. Through this methodology, Part I provided a coded overview across countries of the DPL and its characteristics based on a legal overview of DLA-piper. Coding the law facilitates horizontal comparison between various jurisdictions; the diffusion of information about legal instruments in cyber security. Part I coded characteristics of the DPL that contribute to the notion of 'privacy control'. The results showed that only 5 out of 71 DPLs have penalties for non-compliance that exceed 1 million euro. Also, it revealed that, compared to the United States (US), few countries (21 out of 71) have DBNLs. Furthermore, the research transformed the coded characteristics into an index. Within this index, countries that are not known for their de facto stringent privacy control, such as Mauritius and Mexico, occupy a top position

[632] Which is one of the aims of the research of Part I regarding the role of university.

in this index. Hence, there can be a large difference in the de jure text of the law and the de facto implementation of it. This stresses the need for more empirical research, related to legislation in cyber security. In doing so, Part I directly contributes to the literature of DPLs. A large number of DPLs has emerged the past years across the globe but there has been relatively little academic research to compare them and thus diffuse and unlock information about these laws. Also, Part I contributes to the economics of cyber security literature, since Part I unlocks the 'de jure' text of DPLs for further statistical analysis.

Future research should update and extend the characteristics within the DPL. Yearly updating the coded DPL will result in longitudinal data with information about the laws of various jurisdictions over time. In general, QTA can be extended to a wider number of legal instruments in cyber security, since it facilitates scholars in the economics of cyber security to analyse the effectiveness of these laws on other metrics of cyber security, such as Deep Packet Inspection or spam.[633] Ergo, QTA also contributes to the third ambition of the study; connecting law and economics to the economics of cyber security.

8.1.2 Part II

Part II exemplified the role of government in stimulating information diffusion.[634] Government has the monopoly on violence and the right

---

[633] Van Eeten, Bauer, Asghari et al. (2010).

[634] The reader will maybe note that Part I studied national legislation, which is also adopted by government. However, the criterion for breaking down of the three parts in the study is the role of each of the three parties in stimulating information diffusion. Part I studied the role of university, which can stimulate information about (for instance) governmental legislation in the context of the law and economics of cyber security.

of legislative initiative. The law and economics of cyber security can scrutinize whether these laws (interfering in cyber security) attain their societal goals, for instance information diffusion. From May 26, 2018 onwards, the EU finally has a general data breach notification law as part of the GDPR. Chapter 4 in Part II focused on this piece of legislation, which is potentially capable of contributing to the diffusion of cyber security information. To be precise: Chapter 4 studied whether the EU DBNL is capable of incentivizing private organizations to disclose data of relevant data breaches. In doing so, the analysis took into account a broad range of private and social costs and benefits of data breach disclosure and its regulation. The analysis revealed that most organizations will not spontaneously disclose in the absence of a regulation. This indeed necessitates regulation from a social welfare perspective, provided that solely data breaches that surpass a threshold are disclosed to the public. I concluded that the two main challenges of the EU are 1.) to sufficiently induce organizations to notify and 2.) to set the notification threshold at a socially optimal level. Regarding the former, I argued that solely relying on deterrence will potentially be very costly and/or result in a limited likelihood of detection, even if ex ante risk based auditing or ex post violation specific enforcement are taken into account. I urge the DPA to look at carrots and the expressive function of the law as complementary incentive schemes. Especially the digital first aid kit can be a promising additional incentive for organizations to comply, provided that DPAs developed themselves as a centre of expertise in mitigating data breaches. Regarding the latter (the optimal level of the threshold) my analysis clarified that data breach disclosure can be a costly exercise from a social welfare perspective. Especially notification fatigue and administrative costs of affected individuals negate social benefits when large amounts of insignificant data breaches are being disclosed to the public. Hence, the threshold for notifying to individuals needs to be

fairly high and clear-cut. The threshold for notifying the DPA can be much lower. All in all, the EU DBNL can be a welfare-enhancing piece of legislation provided that it will be enforced and executed wisely by the national DPAs. Consequently, the national DPAs have a crucial role in making the EU DBNL a success. A crucial part of this role is that they should capitalize the techniques and knowledge of the university helix to collect data and perform ex post impact assessments.

8.1.3 Part III

Part III epitomized the role of Industry in stimulating information diffusion. Industry has the contractual freedom that propels the development of innovative products. These innovations can lead to an increase in knowledge diffusion. The law and economics of cyber security can analyse whether and under which conditions these products can contribute to social welfare and information diffusion. Part III focused on two contractual agreements regarding risk shifting. Chapter 5 briefly introduced the theoretical foundations for risk shifting and compared the three forms of risk allocation (individual management, cyber insurance and cyber pooling). It addressed that risk aversion and transaction costs drive the demand for risk shifting. This chapter also discussed the social benefits of the two risk shifting techniques relative to individual risk management. Shifting cyber risk can potentially improve incentives to diffuse information and internalize externalities. Hereafter, Chapter 6 empirically investigated the market for cyber risk insurance contracts. Chapter 7 explored the potential for cyber risk pooling agreements.[635]

---

[635] Faure (2009)

Chapter 6 empirically analysed the developing cyber insurance market and contributed to the law and economics of risk shifting and the literature on cyber insurance. The main advantage of insurance for my endeavour to reduce the information deficit is that insurance facilitates the diffusion of information via a feedback loop between the insurer and the group of insured. In theory, the insurer will accumulate relevant cyber (claim) data and this information will circle back to the insured in the form of advices on how to perform better. Chapter 6 formulated a theoretical framework and observed actual cyber insurance contracts for SMEs in the Netherlands. Some elements in those contracts foster growth of the market, such as simple requesting procedures and the lower prices than several years ago. But in general, a 'catch-22' situation seems to arise in current market for cyber insurance for SMEs. The development of the market is hindered by the information deficit it aims to reduce. First, insurers currently insufficiently focus their coverage on low impact high likelihood risk. Secondly, it is currently hard for most SME to make a well-informed choice regarding which insurance to take. This is either a deliberate sustainment of a market for lemons, or the result of the fact that the development of the market is in an early stage. Also, there are only 2 out of 7 insurers observed that require risk reduction measures. A possible explanation is that there is insufficient information on what these risk reduction measures should entail. Hence, Chapter 6 concludes that the persistent information deficit hampers the efficient development of the cyber insurance market and consequently its contribution in stimulating information diffusion. In order to overcome these challenges, I provided recommendations on future research that could further develop the market. I discussed the alternatives of basic cyber insurance coverage, mandatory disclosure of claim data, a simplified requesting procedure and a clarification of the overlap with property insurance. Last, I stressed the need for

thoroughly analysing the alternatives for traditional insurance, of which Chapter 7 is an example.

Chapter 7 analysed the potential and conditions for using risk pooling as a tool to deal with cyber security risk. Risk pooling has often emerged as an alternative, mostly to insurance, especially for newly emerging risk. Quite surprisingly, there has been only limited attention for risk pooling in cyber security, while cyber security is seen as one of the most important new emerging systemic risk. With newly emerging risk statistical information to allow an accurate pricing of the total risk is often not available and insurer ambiguity may lead to high risk premiums as a result of which there may be no sufficient demand. Chapter 5 on cyber insurance concluded that the persistent information deficit is one of the reasons why the cyber insurance market it still in its infancy.[636] The basic idea with risk pooling is that with cyber risk organizations may have better information than insurers on the risk exposure and the desirable measures to prevent the risk. When this is the case a pool can lead to mutual monitoring, thus stimulating information exchange, a reduction of transaction costs and *ex ante* prevention of risk. I argued that if these conditions are present risk pooling may create protection for individual organizations who participate in the pool, but also positive externalities for society at large since the pool can contribute to the optimal investment in cyber security risk.

---

[636] At the time of writing this synthesis, there are signs that the market for cyber insurance is indeed growing, possibly drive by the GDPR and the recent massive Wannacry and NotPetya attacks.

The main advantage of risk pooling is that it can provide cover even when specific probabilities of an incident occurring remain hard to predict. Whereas insurance always requires a premium setting, pooling is possible without a pricing of the risk. It is necessary, however, to identify the relative contribution of the various participants to the pool. Based on these general starting points I examined the potential of risk pooling for cyber security. I argued that if sufficient information can be gathered by organizations to differentiate the relative risk exposure and contribution of the various participants, the traditional problems of adverse selection and moral hazard (which can equally threaten the emergence of risk pooling) can be remedied.[637] Chapter 7 also noticed that the major advantage of cyber risk pooling would not so much be compensation *ex post* (for which often insurance is used), but rather the information exchange that may be generated through the creation of a pool.

Referring to other examples where risk pools were created, but also where risk pools failed, I pointed at the importance of a careful design of a cyber risk pool. To the best of my knowledge today cyber risk pooling has not yet emerged. However, I argue that there may be a large interest among organizations to create those pools, especially as tools for information diffusion. The emergence of a risk pool, however, requires a correct understanding among organizations of the cyber security risk and some degree of similarity (perhaps even homogeneity) in order to facilitate the risk pooling. It equally requires

---

[637] Adverse selection is exploiting hidden information before the signing of the contract, and moral hazard is exploiting hidden information after the signing of the contract. More about these two classical issues related to risk shifting in Chapter 6, Section 6.2.3 - Section 6.2.5.

an active entrepreneur (like a broker) to initiate the pool. Moreover, risk pooling would never be the only instrument to deal with cyber security, neither as far as prevention, nor as far as compensation is concerned. With respect to compensation a pool would probably include a large deductible as a result of which organizations would still individually manage risk an important part of the loss, also in order to reduce moral hazard. Moreover, pools usually include important limits; the very high (catastrophic) risk is often hedged to (re)insurers. It is therefore likely that in the future cyber risk pooling may take an important place in such a multi-layered 'hybrid' compensation mechanism to deal with cyber security risk.

There are several next steps for future research within the field of risk shifting. The goal of Chapter 6 was to identify, structure and analyse current cyber insurance contracts. In doing so, it was the first identification of insurance contracts for SMEs in the Netherlands. The analysis opened many avenues for future research. One could work on the identification of which risk is suitable for cyber insurance and innovative ways to price this risk in the form of a premium. Also, the consumer side of both cyber insurance and pooling must be explored further, in order to observe their preferences and prerequisites regarding the cyber insurance, but also cyber risk pooling. The goal of Chapter 7 was to sketch that risk pooling could play an important role in cyber security and to show the specific conditions and design issues that would have to be taken into account in developing cyber risk pooling. Of course, the specific nature of the cyber security risk, as well as the different types of cyber risk, does deserve further detailed attention. It may potentially lead to the conclusion that various risk pools have to be created for specific types of cyber security risk. The way in which this can be designed in a more detailed manner as well as the interest of organizations in participation in such a pool are issues

that undoubtedly merit further research. Besides the focus on risk shifting contracts, the research on the role of industry can also identify new innovative contractual solutions for the societal and technical issues in information diffusion. One could for instance think about efficient mechanisms to exchange information at low (marginal cost). In doing so, the research in this field can also benefit from insights obtained from fields in law and economics that dealt with systemic risk, such as nuclear risk, financial risk or environmental risk.

8.2. An Agenda for Stimulating Cyber Security Information Diffusion

It is the studies' second ambition to propose an agenda concerning the stimulation of information diffusion in cyber security for the university, government and industry triple helix. Section 8.2.1 will provide a short recap on the benefits of information diffusion. Section 8.2.2 will discuss the complementary roles, tools and responsibilities of university, government and industry. Section 8.2.3 provides the core recommendations.

8.2.1 The benefits of information diffusion

The study started with the underlying hypothesis that information diffusion can result in more efficient cyber security investments and an increase in social welfare. The following four arguments support the hypothesis.[638]

1. Information diffusion leads to mutual learning regarding efficient cyber security investments. In other words, organizations do not have to reinvent the wheel. Insofar the costs of reinventing the wheel are higher than the costs of

[638] See Chapter 2, Section 2.2.2.

diffusing efficient cyber security investments, this sole argument will lead to a social welfare surplus.

2. The diffusion of cyber security data will lead to better security products. For instance, when information about a vulnerability or a zero day exploits is diffused among security organizations, this will lead an increased pace of patching.[639]
3. Information diffusion reduces market power of big software and security firms. These firms have fewer possibilities for exploiting information asymmetries and the general information deficit. They do this by, for instance, releasing exaggerated cyber security statistics. When the correct information is being diffused, strategic behaviour of these companies will produce little result.
4. When information diffusion reduces transaction costs, this could lead to a reduction of the externalities according to the Coase theorem.[640]

All in all, the study showed that these supporting arguments give sufficient ground for the thesis that the stimulation of information diffusion against affordable social cost is both necessary and as well as indispensable for attaining social welfare in cyber security.

---

[639] However, there can be strong barriers in doing so. For instance, the NSA had insufficient incentives to share its zero day exploit related to the Wannacry virus.
[640] See Chapter 2, Section 2.2.2.

8.2.2 Complementary roles of the triple helix

University, government and industry have complementary roles and tools in the law and economics of cyber security. The simultaneous deployment of these tools yields self-reinforcing innovation.[641]

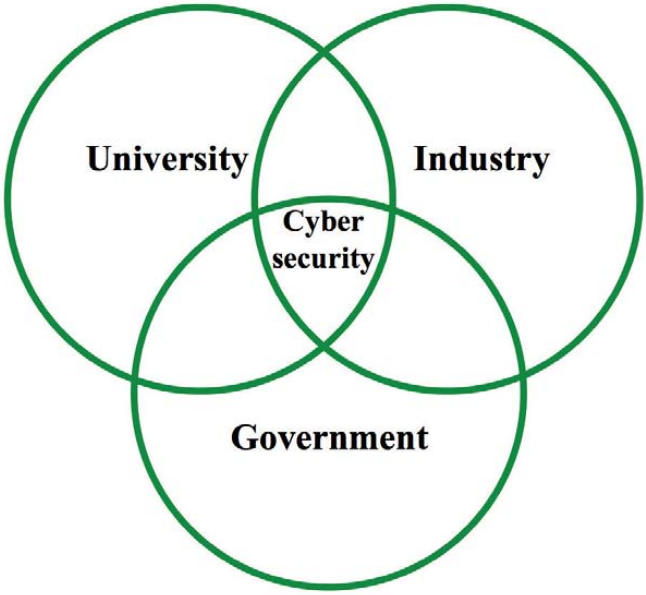


Figure 12: Simultaneously deploying the powers of university, government and industry.

On a high aggregation level, the *University* helix and the scientific methodology can provide the general direction for optimal cyber security investments and attaining cyber security welfare. This study

[641] The analyses of the three substantive parts exemplify this. However, it should be noted that the subjects chosen are just a small subset of the available toolkit that can drive innovation on information diffusion in cyber security in within each helix.

is centralized around one significant section of improvement potential that should be utilized in order to achieve the end of optimal cyber security investments: the stimulation of information diffusion. One aggregation level lower, this study showed that the university helix, and more specifically the law and economics of cyber security, can provide 'stand-alone' research (Part I) but also can assess and provide possibilities for the other helices to contribute to stimulating information diffusion (Part II and III). In other words, the law and economics of cyber security can not only provide the direction for societal effort in cyber security, but can also scrutinize whether actions of the three helices indeed point in such a direction. That is exactly what this study carried out in its substantive parts I, II and III.

Government has the monopoly on violence and the possibility to adopt legislation, which stems from the duty of care to protect its citizens.[642] This legislation, once executed wisely, can potentially contribute to the stimulation of information diffusion. This study scrutinized the case of the DBNL. A DBNL may be able to stimulate information diffusion about data breaches at affordable social cost. In doing so, it also provides additional metrics for cyber security research at universities. Also, the data facilitates risk-shifting agreements that benefit from enhanced information about cyber security. Moreover, the governmental violence monopoly such as the threat of (high) penalties for data breach notifications can drive industry innovation such as the emergence of cyber insurance.

---

[642] Rousseau (1762).

Industry innovation can in itself result in incentives for organizations to better diffuse knowledge. Organizations must innovate in order to survive in a competing world.[643] Innovation that has a societal benefit can drive smart organizational structures or platforms that facilitate and stimulate the de facto stimulation of information diffusion. In doing so, industry has its own unique contribution. For instance, through a risk pooling arrangement, organizations have incentives to disclose data breaches because they have a stake in each other's risk. This has a trickle-down effect to the benefit of university that can use this data for further research studying the microeconomic dynamics of cyber security by using the academic methodology. Industry innovation can drive compliance with regulation from the government helix the other way around. Part III showed that when an organization is covered by cyber insurance or through a cyber risk pool, it is less painful to comply with data breach notification legislation, because some damages related to the disclosure of notifications are covered.

8.2.3 Recommendations

The study provides examples of how the different tools of the three different parts of society can be utilized. The studies' deep dives show that the specific tools of university, government and industry can be deployed much broader. How should an agenda for the triple helix

---

[643] Some say that in a purely capitalist society, *Industry* will act in its own interest and will only act insofar these actions directly contributes to its own return on investment. For some critical comments, see Marx and Engels (1848). But still, industry is bound by the harm principle, which could reach far in the case of cyber security because of the interdependence of computer systems. In addition, social factors like Corporate Social Responsibility (CSR) policy can influence organizations to innovate beyond what is directly profitable for them.

emerge? And in what way will the joint deployment of their individual tools produce the most fruitful results? 'Awareness' and 'cooperation' are two important building blocks, as this section will argue.

Awareness. Each helix should be aware of its unique role and responsibility in the simulation of cyber security information diffusion. With regards to the government and industry helices, the scope of diffusion determines whether either government or industry has a primary role in executing it.[644] This government-industry dyad also touches upon the political question of solving societal problems by either centralized regulation or 'laisser faire' (by contractual agreements in) the market. With respect to the latter, industry should be made aware that certain types of innovations in cyber security (for instance in the sphere of risk shifting) yield more social welfare than others. Government can assist industry by subsidizing or promoting the start-up costs of innovations that are socially beneficial. Last, the university helix should be able to study the role of all three parties in the triple helix and should be able to diffuse information where there is special knowledge or techniques needed before information can be diffused. The upcoming Section 8.3 will point out that a further connection between law and economics and economics of cyber security will benefit this distinguished role of university.

Cooperation. Each party in the triple helix has its own role and responsibility. However, the nexus between the three parties will grow stronger when they are able to engage in mutual understanding. A deep and sustainable cooperation between the helices should emerge regarding information diffusion and pressing social challenges in

---

[644] See Chapter 2, Section 2.5.1.

cyber security. For instance, university should cooperate with government and industry to scrutinize the social benefits of their actions. This academic study showed that such an analysis of the three parties through the lenses of university party can yield fruitful results.[645] Government and industry also should further enhance public-private information diffusion, not only for large organizations, but also for SMEs.[646]

8.3. The Law and Economics of Cyber Security

The study applied law and economics to cyber security. Hence, the fields of *law and economics* and *economics of cyber security* acted on the stage of the study. Both disciplines use microeconomics to study the dynamics of either the law or cyber security. However, there has been little research on cyber security in law and economics[647] and there has been relatively little research on the role of the law and legal instruments in the economics of cyber security.[648] This section will

---

[645] See Chapter 2, Section 2.5.

[646] See also Cyber Security Council (2017) < https://www.cybersecurityraad.nl/binaries/CSR-advies%202017%20nr.%202%20-%20Naar%20een%20landelijk%20dekkend%20stelsel%20van%20informatieknooppunten_tcm56-269317.pdf> (accessed 30 March 2018).

[647] Law and Economics scholars Grady and Parisi (2005) bundled essays on cyber security, but these essays did not include the microeconomic focus of the Economics of Cyber Security.

[648] This does not withstand the fact that there is literature within the economics of cyber security research that included the law. For instance, the effects of the adoption of data breach notification laws have been measured by relating them to identity theft rates (Romanosky, Telang and Acquisti (2011), pp. 256-286). These laws have been subject to further evaluation, for instance by Bisogni (2013). Furthermore, the membership of cybercrime convention of different countries has been correlated with the amount of spam at ISP's in these countries (Van Eeten et al. ((2010). Also, the economics and regulation of certification authorities have

briefly identify how this study contributed to the connection of the two fields (8.3.1), the barriers that caused this insufficient connection (8.3.2). Research in the law and economics of cyber security has large relevance and impact and should strive to maximize its societal utility.[649] Accordingly, when scholars from either law and economics or the economics of cyber security choose to perform research in the area of law and economics of cyber security they should utilize the knowledge from the other field. Section 8.3.3 provides recommendations for fostering its further linkage.

8.3.1 Connecting the two fields in this study

It is the studies' third ambition to make a first step in the connection of law and economics with the economics of cyber security.[650] On the one hand, the study familiarized scholars of the economics of cyber security with the application of law and economics methodology to issues in cyber security. The QTA in Part I disclosed DPLs for quantitative research in the economics of cyber security. The doctrine of optimal enforcement in Part II was the fundament for the analysis on better DBNLs. Part III introduced the law and economics of risk shifting, and through its extensive theoretical foundations it was possible to identify conditions for so-called hybrid structures where individual risk management, cyber insurance and pooling can play a

---

been researched (Arnbak, Asghari, Van Eeten et al. (2014)) A last example is research on the cross-country independence of cyber attacks (Wang and Kim, (2009)).

[649] As of 2014, this also happens to be the slogan of Rotterdam University (Management Bulletin (2017) < https://www.eur.nl/sites/corporate/files/_140041-01_EUR_middelen_nieuwe_strategie_folder_fase3_08.pdf> (accessed 30 March 2018).

[650] Also called the Economics of Information Security or EconInfoSec. See www.econinfosec.org

role. In doing so, the research capitalized on the fact that many concepts in law and economics have been valuable in other areas of law and economics, such as the insights from risk pooling contracts applied to cyber security in Part III. On the other hand, the study acquainted the scholars in law and economics with the key insights from the economics of cyber security. This includes the core dynamics of investing in cyber security, such as threats, vulnerability, impact and strategies to reduce them. It also provided an introduction into the specific microeconomic peculiarities of the systemic cyber security risk, such as far reaching externalities, various types of stubborn information deficits and persistent market power of security and software companies.

All in all, the study aims to inspire future researchers in either field to work at these crossroads. Without a doubt, the intersection of law and economics and economics of cyber security is fertile ground for contributing to optimal cyber security. When legal instruments are entering the cyber security theatre, scholars of law and economics and the economics of cyber security should work together in order to make sure they contribute to social welfare or at least show what the social welfare implications of these choices are. And within the context of the storyline of the study, the law and economics of cyber security should design and analyse legal instruments that contribute to information diffusion.

8.3.2 Barriers to building the bridge

So far I discussed the advantages of the further connection of law and economics with the economics of cyber security. The analysis in Chapter 1, Section 1.2.1 revealed that mutual referencing to both disciplines is solely 3-4% of total references of a paper, when subjects in one field are discussed are discussed that largely overlap with this

other discipline (either legal or cyber security). The question naturally arises *why* the two fields did not connect sufficiently. This section poses the 'opposite tradition' hypothesis that I developed over the past years, while performing research on the intersection of both disciplines.[651] The differences in tradition between law and economics and economics of cyber security are displayed in Table 35 below.

Table 35: Differences in tradition between law and economics and economics of cyber security

Law and economics	**Economics of cyber security**
Started in 1960s	Started in the 2000s
Theory first	Empirics first
Deductive reasoning	Inductive reasoning
Formal and slow publication culture	Informal and fast publication culture

Law and economics is an almost classical movement that puts the development of theory as a primary paramount principle. This also stems from the fact that law and economics applies the economic analysis to the law in order to load the latter with the necessary theory. Ronald Coase, one of the founders of the movement and winner of the Nobel Prize in Economics, liked to stress that: "much legal scholarship

[651] Amongst others, In 2014, I took several courses in Law and Economics at Bologna and Hamburg University. Hereafter, in pursuing the PhD endeavor, I participated and attended conferences such as the Annual Conference of the European Association of Law, Economics and the Workshop of Economics of Information Security and the Rotterdam EDLE seminar series 2015-2016. I also collaborated with the economics of cyber security department at Delft University, mainly on the research in Chapter 3 and Chapter 6.

is not much more than 'stamp collection'."[652] He meant that legal scholarship mostly concerns classifying and organizing legal structures, or as he liked to call it, "operating a file system".[653] Without a theoretical framework, such as the one that law and economics aims to develop and provide, there is indeed little analysis and synthesis in legal scholarship. The theoretical framework from which law and economics aims to depart implicates that there is general a deductive method to come to logical conclusions. Academic insights in the Law and Economics movement are shared in many well-read key journals.[654] This formal publication culture has the advantage of thorough scrutiny but can also hinder the dissemination of knowledge in the rapidly changing analysis of cyber security.

Economics of cyber security is a much younger field that many believed had its genesis in 2001 by a seminal article of Ross Anderson.[655] Anderson is originally a computer scientist. Accordingly, the culture of the economics of cyber security arguably has some of the 'trial and error' approach of developing software code. This is also related to the ascertainment that there is still limited data available about the cyber security market.[656] The majority of the papers presented at its main forum WEIS do have a significant empirical component. For instance, within the 2017 edition of WEIS, I observed a significant empirical

---

[652] Coase (1992), p. 254
[653] Coase (1992), p. 254..
[654] For instance, the Quarterly journal, Journal of Law and Economics, the Journal of Empirical Studies, the Journal of law and economics, the RAND Journal of Economics, the Journal of Law, Economics, & Organization, the Journal of Legal Studies, the Journal of Legal Studies and the International Review of Law and Economics.
[655] Anderson (2001).
[656] Anderson, Böhme, Clayton et al. (2008).

component in 18 out of the 23 papers that were presented. Hence, the inference can be made that within the economics of cyber security, collecting and analysing empirical data is paramount. The empirical data is being used to analyse in what way microeconomic dynamics may be in play in several subsets of cyber security and cybercrime markets. The inductive reasoning of the economics of cyber security is much more pragmatic than law and economics. This is also reflected in the fact that publications at its main annual conference WEIS have the status of a published article in a journal, which naturally greatly enhances information diffusion since the time from submission to publication and presentation at WEIS could be as short as four months.

The differences between the two disciplines are not necessarily detrimental. As long as the differences are not unbridgeable, they allow the two disciplines from mutual learning for the benefit of science and society.[657] There is certainly a possibility for mutual learning, because both disciplines use microeconomics as their core methodological toolkit.

8.3.3 Recommendations

The benefits of connecting law and economics with the economics of cyber security are large but there is an equally large gap to be bridged. Without mutual understanding of the different traditions, the risk arises that the quality for the one can be a detriment for the other. In that situation, the economics of cyber security cannot benefit from the

[657] See for a nice example to bridge the gap between the Internet measurement of the economics of cyber security and other policy fields: Asghari, van Eeten and Mueller (2013).

vast theoretical development of law and economics and the dynamics of cyber security will not be opened for law and economics scholars.[658] A considerable effort needs to be made to connect these fields.

It is indispensable that scholars in both fields want to cooperate and learn from each other. Parties must see the social benefits for university and society of this cooperation. This means that a vision of connecting the law and economics with the economics of cyber security and its contribution to science and society should be developed. Both fields should endorse the joint goal and building blocks of the law and economics of cyber security: the optimizing or clarification of legal instruments through microeconomic analysis in order for them to contribute to optimal cyber security. Private incentives can be increased if cooperation leads to a positive individual reward, for instance a positive impact on individual academic careers. For instance, there must be space for contributions related to cyber security in high impact law and economics journals and vice versa. For this, it is necessary that parties know how to utilize its each other's field and how to find each other. This means that there should be accessible and efficient information exchange between the fields.

Last, scholars in both disciplines must have basic knowledge of the other disciplines. For instance, one could embed law and economics courses in cyber security education and cyber security courses in law and economics education. There must be leadership in making and sustaining the connection and setting up structures to meet and share knowledge, both offline and online. As said, the traditions of the two fields differ and in that sense, mutual respect for each other's traditions

---

[658] See for an overview: Cooter and Ulen (2016).

can foster cooperation and these structures will build mutual trust on an individual level. This can be done through for instance joint authorship, symposia and journals. Last, evaluation and feedback mechanisms that enable continuous learning about the integration of the fields are crucial for its development.

8.4. Closing Remarks

This play in the cyber security theatre has almost finished. I will provide the reader with some closing remarks, before the curtain falls. To put it a little bit bluntly: Within cyber security, one could argue that traditional microeconomic theory has taken steroids. The interwovenness of digital devices amplify and turbocharge misaligned incentives, information deficits and other market failures. Legal instruments can get through this steroid storm and eventually re-align incentives to increase information diffusion and social welfare.[659] But in order to fulfil this promise, law and economics must gain a deeper link to the economics of cyber security. This *law and economics of cyber security* has the task to further formulate common 'cyber security information diffusion' agenda for university, government and industry. The law and economics of cyber security could engage in information diffusion *about* legal instruments and scrutinize initiatives of government and industry to diffuse information *through* legal instruments. This study took a first step in doing so.

The further integration of our analogue lives with the digital world will inevitably continue. So will its downsides, in the near and distant

---

[659] Here I will end the metaphor since otherwise there will be too much overlap with medical sciences (Moumli, Valk, Sanson-van Praag and Zelissen (2012)).

future.[660] The Internet has brought us unprecedented prosperity and empowerment.[661] The law and economics of cyber security can provide a foundation for good times in our lifetime and the ages to come.

Plaudite, amici, comedia finita est.

[660] For the very distant future, it might be interesting to read the literature related to quantum computing and its impact on traditional encryption.
[661] Analysts estimate that the Internet accounts for 21% GDP growth in developed economies between 2006 and 2011 (Pélissié du Rausas (2011)).

BIBLIOGRAPHY

Bibliography

Gwen Ackerman, 'G-20 Urged to Treat Cyber-Attacks as Threat to Economy' *The Seattle Times* (Seattle, 14 June 2013) <http://www.seattletimes.com/business/g-20-urged-to-treat-cyberattacks-as-threat-to-global-economy/> accessed 30 March 2018.

J. Akella, S. Marwaha and J. Sikes, 'How CIOs can lead their company's information business' (2014) 2 McKinsey Quarterly.

George Akerlof, 'The Market for Lemons' (1970) 84 Quarterly Journal of Economics 488.

Ross J. Anderson, 'Why Information Security is Hard – An Economic Perspective' (University of Cambridge 2001) <http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf> accessed 30 March 2018.

Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd edn, Wiley 2008).

Ross J. Anderson, *Security Engineering* (2nd edn, Wiley 2010).

R. Anderson, C. Barton, R. Bohme, R. Clayton, M.J.G. van Eeten, M. Levi, T. Moore and S. Savage, 'Measuring the Cost of Cybercrime' (Workshop on Economics of Information Security 2012) <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf> accessed 30 March 2018.

Ross J. Anderson, R. Böhme, R. Clayton and T. Moore, 'Security Economics and the Internal Market' (*ENISA*, 31 January 2008) <http://www.enisa.europa.eu/publications/archive/economics-sec> accessed 30 March 2018.

Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore and Stefan Savage, 'Measuring the Cost of Cybercrime' in Rainer Böhme (ed), *The Economics of Information Security and Privacy* (Springer 2013).

Ross J. Anderson and Tyler Moore, 'Information Security Economics – and Beyond' (9th International Conference on Deontic Logic in Computer Science, Luxembourg, 2008) <https://www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf> accessed 30 March 2018.

A.M. Arnbak, *Securing private communications: protecting private communications security in EU law - fundamental rights, functional value chains, and market incentives* (Kluwer Law International 2016).

A. Arnbak and N. van Eijk, 'Certificate Authority Collapse, Regulating Systemic Vulnerabilities in the HTTPS Value Chain' (2012) TRPC <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031409> accessed 30 March 2018.

Kenneth J. Arrow, 'Uncertainty and the Welfare Economics of Medical Care' (1963) 53 American Economic Review 941.

Kenneth J. Arrow, *Social Choice and Individual Values* (2nd edn, Yale University Press 1963).

Hadi Asghari, Michel J.G. van Eeten and Johannes M. Bauer, 'Economics of cybersecurity' in Johannes M. Bauer and Michael Latzer (eds), *Handbook on the Economics of the Internet* (Edward Elgar Publishing 2016).

Hadi Asghari, Michel J.G. van Eeten and M. L. Mueller. 'Unravelling the Economic and Political Drivers of Deep Packet Inspection' (GigaNet 7th Annual Symposium, Baku, November 2012).

Hadi Asghari, Michel J.G. van Eeten and Milton L. Mueller, 'Internet Measurements and Public Policy: Mind the Gap' (Proceedings of the 6th USENIX Conference on Cyber Security Experimentation and Test, 2013) <https://www.usenix.org/system/files/conference/cset13/cset13-asghari.pdf> accessed 30 March 2018.

Terrence August and Tunay I. Tunca, 'Comments on Incentives To Adopt Improved Cybersecurity Practices' (National Telecommunications & Information Administration 2013).

I. Ayres and J. Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

Walter S. Baer and Andrew Parkinson, 'Cyberinsurance in IT Security Management' (2007) 5(3) IEEE Security & Privacy 50.

Liam M.D. Bailey, 'Mitigating Moral Hazard in Cyber-Risk Insurance' (2014) 3(1) Journal of Law & Cyber Warfare 1.

Baker Law, 'International Compendium of Data Privacy Laws' (Baker Law 2014).

K. A. Bamberger and D. K. Mulligan. 'Privacy in Europe: Initial Data on Government Choices and Corporate Practices' (2013) 81(5) George Washington Law Review 1529.

Tridib Bandyopadhyay, Vijay S. Mookerjee and Ram C. Rao, 'A Model to Analyze the Unfulfilled Promise of Cyber Insurance: The Impact of Secondary Loss' (2004) University of Texas, TX Working paper <http://www.utdallas.edu/~rrao/CyberBMR%5B1%5D.pdf > accessed 30 March 2018.

Tridib Bandyopadhyay, Vijay S. Mookerjee and Ram C. Rao, 'Why IT Managers Don't Go for Cyber-Insurance Products' (2009) 52(11) Communication of the ACM 68.

Courtney A. Barclay, 'A comparison of proposed legislative data privacy protections in the United States' (2013) 29(4) Computer Law & Security Review 359.

Francis M. Bator, 'The Anatomy of Market Failure' (1958) 72(3) Quarterly Journal of Economics 351.

Johannes M. Bauer and Michel J.G. van Eeten, 'Cybersecurity: Stakeholder incentives, externalities, and policy options' (2009) 3(10-11) Telecommunications Policy 706.

D.L. Baumer, J.B. Earp and J.C. Poindexter, 'Internet privacy law: a comparison between the United States and the European Union' (2004) 23(5) Computer Security 400.

G.S. Becker, 'Crime and Punishment: An Economic Approach' (1968) 76(2) The Journal of Political Economy 169.

Naomi Bekker, 'UPDATE: Gate open 24/7 this weekend for truck import (pick up) and export (delivery) at APM Terminals Rotterdam' (APM Terminals Rotterdam, 2 July 2017) <https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693> accessed 30 March 2018.

P. Bennet, 'Mutual risk: P&I Insurance Clubs and Maritime Safety and Environmental Performance' (2001) 25 Marine Policy 13.

Jeremy Bentham, *An Introduction tot he Principles of Morals and Legislation* (London: Mewsgatt Charing Cross 1789).

Abram Bergson, 'A Reformulation of Certain Aspect of Welfare Economics' (1938) 52(2) Quarterly Journal of Economics 310.

Baruch Berliner, *Die Grenzen der Versicherbarkeit von Risiken* (Zürich: Schweizerische Rückversicherungsgesellschaft 1982).

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 30 March 2018.

Richard S. Betterley, 'Cyber/Privacy Insurance Market Survey 2013, The Betterley Report' (2013)

<http://betterley.com/samples/cpims13_nt.pdf> accessed 30 March 2018.

Christian Biener, Martin Eling and Jan Hendrik Wirfs, 'Insurability of Cyber Risk: An Empirical Analysis' (2015) 40(1) Geneva Papers on Risk and Insurance 131.

Biometric Technology Today. 'Global data protection authorities tackle Google on Glass privacy' (2013) 2013(7) Biometric Technology Today 1.

F. Bisogni, 'Data Breaches and the Dilemmas in Notifying Customers' (Fourteenth annual Workshop on the Economics of Information Security (Workshop on Economics of Information Security, Delft, 2015)
<http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_bisogni.pdf> accessed 30 March 2017.

R. Böhme and G. Kataria, 'Models and Measures for Correlation in Cyber-Insurance' (Fifth Annual Workshop on the Economics of Information Security, University of Cambridge, 2006)
<http://www.econinfosec.org/archive/weis2006/docs/16.pdf> accessed 30 March 2018.

R. Böhme and G. Schwarz, 'Modelling cyber-insurance: Towards A Unifying Framework' (Ninth Annual Workshop on the Economics of Information, Boston, 2010)
<http://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf> accessed 30 March 2018.

P. Boillat and M. Kjaerum, *Handbook on European data protection law* (Publication Office of the European Union 2014).

Arjen Boin and Michel van Eeten, 'The Resilient Organization' (2013) 15(3) Public Management Review 429.

G.E.P. Box and N.R. Draper, *Empirical Model Building and Response Services* (John Wiley and Sons 1987).

Sarah Breitenbach, 'States at odds with feds on data breach proposals' (Stateline, 12 June 2015) <http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/6/12/states-at-odds-with-feds-on-data-breach-proposals> accessed 30 March 2018.

Alexander Brem and Agnieszka Radziwon, 'Efficient Triple Helix collaboration fostering local niche innovation projects – A case from Denmark' (2017) 123 Technological Forecasting & Social Change 130.

J.P. Brown, 'Toward an Economic Theory of Liability' (1973) Journal of Legal Studies 323.

Mark de Bruijne and Michel van Eeten, 'Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment' (2007) 15(1) Journal of Contingencies and Crisis Management 18.

H. Buhlmann and W.S. Jewell, 'Optimal Risk Exchanges' (1979) 10 Astin Bulletin 243.

Mark Burdon, Jason Reid, Rouhshi Low, 'Encryption safe harbours and data breach notification laws' (2010) 26(5) Computer Law and Security Report 520.

E.J. Byres and J. Lowe, 'The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems' (VDE Congress, October 2014).

Albert Caballero, *Computer and Information Security Handbook* (Morgan Kaufmann Publications. Elsevier inc. 2009) ch 14.

Guido Calabresi, *The Costs of Accidents: A Legal and Economics Analysis* (Yale University Press 1970).

Guido Calabresi, 'The Pointlessness of Pareto: Carrying Coase Further' (1991) 100(5) Yale Law Journal 1211.

H. Cavusoglu, B. Mishra and S. Raghunathan, 'The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers' (2004) 9(1) International Journal of Electronic Commerce 69.

James J. Cebula and Lisa R. Young, 'A Taxonomy of Operational Cyber Security Risks' (Software Engineering Institute, Carnegie Mellon University 2010) < https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395> accessed 30 March 2018.

CERT-UK and GCHQ, 'Common Cyber Attacks: Reducing the Impact' (UK: Crown 2015).

Orcun Cetin, Carlos Ganán, Maciej Korczynski and Michel van Eeten, 'Make Notifications Great Again: Learning How to Notify in the Age

of Large-Scale Vulnerability Scanning' (16th Annual Workshop on Economics of Information Security, La Jolla, 2017) <http://mkorczynski.com/WEIS2017Cetin.pdf> accessed 30 March 2018.

Jennifer A. Chandler, 'Liability for Botnet Attacks' (2006) 5 (1) Canadian Journal of Law and Technology 13.

H.F. Chang, 'A Liberal Theory of Social Welfare: Fairness, Utility, and the Pareto Principle' (2000) 110(2) The Yale Law Journal 173.

L. Cheng, Ying Li, Wenli Li and Qingguo Zhai, 'Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory' (2013) 39 Computer & Security 447.

Pierre-André Chiappori and Bernard Salanié, 'Testing for Asymmetric Information in Insurance Markets' (2000) 108(1) Journal of Political Economy 56.

W.B. Chik, 'The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform' (2013) 29(5) Computer Law & Security Review 554.

David Chinn, James Kaplan and Allen Weinberg, 'Risk & responsibility in a hyperconnected world: Implications for enterprises' (Report McKinsey&Company 2014).

Carl von Clausewitz, *Vom Kriege* (1832).

R. Clayton and T. Mansfeld, 'A Study of Whois Privacy and Proxy Server Abuse' (13th Annual Workshop on the Economics of Information Security, Pennsylvania State University, 2014) <https://www.cl.cam.ac.uk/~rnc1/whoisstudy.pdf> accessed 30 March 2018.

I. Cofone, 'The Value of Privacy: Keeping the Money Where the Mouth is' (Fourteenth annual Workshop on the Economics of Information Security, Delft, 2015) <http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_cofone.pdf> accessed 30 March 2018.

Robert D. Cooter, 'Expressive law and economics' (1998) 27 Journal of Legal Studies 585.

Robert D. Cooter, 'Do good laws make good citizens? An economic analysis of internalized norms' (2000) 86 Virginia Law Review 1577.

Robert D. Cooter and Thomas Ulen, *Law and Economics* (4th edn, Pearson Addison-Wesley 2004).

Robert D. Cooter and Thomas Ulen, *Law and Economics* (6th edn, Pearson Addison-Wesley 2016).

Louis Anthony Cox, 'Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks' (2008) 28(6) Risk Analysis 1749.

Matthew Crane, 'International Liability in Cyberspace' (2001) 1 Duke Law & Technology Review.

Cyber Security Raad, 'Naar een landelijk dekkend stelsel van informatieknooppunten: advise inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime' (CSR-advies 2017 nr. 2).

G. Dari-Mattiaci and G. de Geest, 'Carrots, sticks, and the multiplication effect' (2010) 26 Journal of Law, Economics, and Organization 365.

N. Doherty and G. Dionne, 'Insurance with Undiversifiable Risk: Contract Structure and Organizational Form of Insurance Firms' (1993) 6 Journal of Risk and Uncertainty 173.

Dutch Network Group, 'Grip op Cybercrime in Ondernemend Nederland' (2016) <http://www.dutchnetworkgroup.com/2878/grip-cybercrime-ondernemend-nederland.htm> accessed 30 March 2018.

Andrew Dyson, Jim Halpert, Diego Ramos, Richard van Schaik, Scott Thiel, Carol A.F. Umhoefer and Patrick van Eecke, 'Data Protection Laws of the World Handbook' (3rd edn, DLA Piper 2014).

Benjamin Edwards, Steven Hofmeyr and Stephanie Forrest, 'Hype and Heavy Tails: A Closer Look at Data Breaches' (14th Annual Workshop on Economics of Information Security, Delft, 2015) <http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_edwards.pdf> accessed 30 March 2018.

Michel J.G. van Eeten and Johannes M. Bauer, 'Economics of Malware: Security Decisions, Incentives and Externalities' (2008) STI Working Paper 1/2008.

Michel van Eeten, Johannes M. Bauer, Hadi Asghari and S. Tabatabaie, 'The Role of Internet Service Providers in Botnet Mitigation: an Empirical Analysis based on Spam Data' (2010) OECD STI Working Paper 2010/5.

Michel J.G. van Eeten and M. Mueller, 'Where is the Governance in Internet Governance' (2013) 15(5) New Media & Society 720.

Isaac Ehrlich and Gary S. Becker, 'Market Insurance, Self-Insurance, and Self-Protection' (1972) 80(4) Journal of Political Economy 623.

S. Elahi, 'Privacy and consent in the digital era' (2009) 14(3) Information Security Technical Report 113.

M. Eling and W. Schnell, 'Ten Key Questions on Cyber Risk and Cyber Risk Insurance' (Geneva: The Geneva Association 2016) <https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf> accessed 30 March 2018.

ENISA, 'Incentives and Barriers of the Cyber Insurance Market in Europe' (Report for the European Commission, 2012).

H. Etzkowitz, 'Technology transfer: The second academic revolution' (Technology Access Report 1993).

H. Etzkowitz and L. Leydesdorff, 'The Triple Helix: University – Industry – Government Relations: A Laboratory for Knowledge-Based Economic Development' (1995) 14 EASST Review 14.

H. Etzkowitz and L. Leydesdorff, 'The dynamics of innovation: from National Systems and "Mode 2" to a Triple Helix of university-industry-government relations' (2000) 29 Research Policy 109.

Michael G. Faure, 'Alternative Compensation Mechanisms as Remedy for Uninsurability of Liability' (2004) 29(3) The Geneva Papers on Risk and Insurance 455.

Michael G. Faure, *Tort Law and Economics* (Edward Elgar Publishing 2009).

Michael G. Faure, 'In the Aftermath of the Disaster: Liability and Compensation Mechanisms as Tools to Reduce Disaster Risks' (2016) 52(1) Stanford Journal of International Law 95.

Michael G. Faure and K. Fiore, 'The coverage of the nuclear risk in Europe: Which Alternative?' (2008) 33 The Geneva Papers on Risk and Insurance – Issues and Practices 288.

Michael G. Faure and T. Hartlief, 'Insurance and expanding systemic risks' (Paris: OECD 2003).

Michael G. Faure, J. Liu and H. Wang, 'A multilayered approach to cover damage caused by offshore facilities' (2015) 33 Virginia Environmental Law Journal 356.

Michael G. Faure and Bernold F.H. Nieuwesteeg 'The Law and Economics of Cyber Risk Pooling' (2018) New York University Journal of Law and Business (forthcoming).

Michael G. Faure and D. Porrini, 'Göran Skogh on Risk Sharing and Environmental Policy' (2017) 42(2) The Geneva Papers on Risk and Insurance – Issues and Practice 177.

Michael G. Faure and H. Wang, 'Compensating Victims of a European Deepwater Horizon Accident: OPOL Revisited' (2015) 62 Marine Policy 25.

Financieel Dagblad, 'Fraude met internetbankieren 'spectaculair gedaald'' *Financieel Dagblad* (15 September 2016) <https://fd.nl/economie-politiek/1167515/fraude-met-internetbanken-spectaculair-gedaald> accessed 30 March 2018.

Jessica Fino, 'Vast Majority of SMEs Vulnerable to Cyber Attacks and IT Threats, Survey Finds' (2016) <http://economia.icaew.com/news/july-2016/smes-vulnerable-to-cyber-attacks-and-it-threats> accessed 30 March 2018.

D. Frisch and J. Baron, 'Ambiguity and Rationality' (1988) 1(3) Journal of Behavioral Decision Making 149.

Huw Fryer, Roksana Moore and Tim Chown, 'On the Viability of Using Liability to Incentivise Internet Security' (Workshop on Economics of Information Security, Georgetown University, 2013) <http://www.econinfosec.org/archive/weis2013/papers/FryerMooreChownWEIS2013.pdf> accessed 30 March 2018.

José M. de Fuentes, Lorena González-Manzano, Juan Tapiador and Pedro Peris-Lopez 'PRACIS: Privacy-preserving and aggregatable cybersecurity information sharing' (2017) 69 Computers & Security 127.

Marc Galanter, 'Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change' (1974) 1974(9) Law and Society 95.

G. de Geest and G. Dari-Mattiacci, 'The Rise of Carrots and the Decline of Sticks' (2013) 80(1) University of Chicago Law Review 341.

Ties Gijzel, 'Ziek en zelfstandig? Dan is een broodfonds misschien iets voor jou' *NRC* (Amsterdam, 23 March 2016) <https://www.nrc.nl/nieuws/2016/03/22/nrc-q-ziek-en-zelfstandig-dan-is-een-broodfonds-misschien-iets-voor-jou-a1493495> accessed 30 March 2018.

Edward M. Glaser, Harold H. Abelson and Kathalee N. Garrison, *Putting Knowledge to Use: Facilitating the Diffusion of Knowledge and the Implementation of Planned Change* (Jossey-Bass Publishers 1983).

S. Goel and H. Shawsky, 'Estimating the market impact of security breach announcements on firm values' (2009) 46(7) Information and Management 404.

L.A. Gordon, M.P. Loeb and W. Lucyshyn, 'Sharing information on computer systems security: an economic analysis' (2003) 22(6) Journal of Accounting and Public Policy 461.

L.A. Gordon, M.P. Loeb, W. Lucyshyn and L. Zhou, 'The impact of information sharing on cybersecurity underinvestment: A real options perspective' (2015) 34(5) Journal of Accounting and Public Policy 509.

Graig and the Burca, *EU Law: Text, Cases and Materials* (Oxford University Press 2015).

H. Grant, 'Data protection 1998–2008' (2009) 25(1) Computer Law & Security Review 44.

G. Greenleaf, 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108' (2012) 2(1) International data privacy law.

G. Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories' (2014) 23(1) Journal of Law, Information and Science 4.

Judy Greenwald, 'Financial institutions identify cyber risk as major concern: Survey' *Business Insurance* (23 October 2014) <http://www.businessinsurance.com/Article/20141023/NEWS07/141029882> accessed 30 March 2018.

Mark Greisiger, 'Cyber Liability & Data Breach Insurance Claims – A Study of Actual Payouts for Covered Data Breaches' (PA: NetDilligence, 2011).

S. Grossmann and M.G. Faure, 'Conditions for effective risk sharing against marine pollution: the case of the Ria de Vigo, NW Spain' (2016) 24(2) Environmental Liability 59.

A. Haas and A. Hofmann, 'Risiken Aus Cloud-Computing-Services: Fragen Des Risikomanagements Un Aspecte Der Versicherbarkeit' (2013) FZID Discussion Paper 74/2013 <http://opus.uni-

hohenheim.de/volltexte/2013/853/pdf/fzid_dp_2013_74_Schiller.pdf> accessed 30 March 2018.

Yacov Y. Haimes, 'On the Definition of Vulnerabilities in Measuring Risks to Infrastructures' (2006) 26(2) Risk Analysis 293.

Harvard Business Review, 'Meeting the cyber risk challenge' (2012) < https://hbr.org/2012/12/meeting-the-cyber-risk-challen.html> accessed 30 March 2018.

Trey Herr and Sasha Romanosky, 'Cyber Crime: Security Under Scarce Resources' (AFPC 2015).

P. de Hert and V. Papakonstantinou, 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 Computer Law and Security Review 179.

J.R. Hicks, 'The Foundations of Welfare Economics', (1939) 49 The Economic Journal 696.

Annette Hofmann and Hidajet Ramaj, 'Interdependent Risk Networks: The Threat of Cyber Attack' (2011) 11(5-6) International Journal of Management and Decision Making 312.

R. Hogarth and H. Kunreuther, 'Ambiguity and Insurance Decisions' (1985) 75 American Economic Review 386.

B. Holstrom, 'Moral Hazard In Teams' (1981) Working paper, Northwestern University, Illinois <https://www.kellogg.northwestern.edu/research/math/papers/471.pdf> accessed 30 March 2018.

C.A. Holt and S.K. Laury, 'Risk Aversion and Incentive Effects' (2002) 92(5) American Economic Review 1644.

Insureon, 'Target's Cyber Liability Insurance Covered 36% of Its Data Breach Costs. How Much Does Yours Cover?' (24 March 2015) <http://www.insureon.com/blog/post/2015/03/24/how-much-does-your-cyber-liability-insurance-cover.aspx> accessed 30 March 2018.

Inga A. Ivanova and Loet Leydesdorff, 'Rotational symmetry and the transformation of innovation systems in a Triple Helix of university-industry-government relations' (2014) 86 Technological Forecasting & Social Change 143.

Robert H. Jerry II and Michele L. Mekel, 'Cybercoverage for Cyber-Risks: An Overview of Insurers' Responses to the Perils of E-Commerce' (2001) 8 Connecticut Insurance Law Journal 7.

M. Jus, *Credit Insurance* (Oxford: Elsevier 2013).

Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47(2) Econometrica 263.

Daniel Kahneman and Amos Tversky, 'On the Reality of Cognitive Illusion' (1996) 103(3) Psychological Review 582.

Nicholas Kaldor, 'Welfare Propositions of Economics and Interpersonal Comparisons of Utility' (1939) 49 The Economic Journal 549.

T. Kayworth, L. Brocato and D. Whitten. 'What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles' (2005) 16(6) Communications of the Association for Information Systems 110.

J.P. Kesan, M.P. Ruperto and W.J. Yurcik, 'The Economic Case for Cyberinsurance' (2004) Working paper, University of Illinois, IL.

M. Ko and C. Dorantes, 'The impact of information security breaches on financial
performance of the breached firms: an empirical investigation' (2006) 16(2) Journal of Information
Technology Management 13.

Jan de Kok, Yvonne Prince and Tommy Span, *De bijdrage van het MKB aan de Nederlandse economie* (Zoetermeer: Panteia 2015).

D. Korff and I. Brown, 'New Challenges to Data Protection - Final Report' (European Commission DG Justice 2010).

R.B. Korobkin and T.S. Ullen, 'Law and Behavioral Science: Removing the Rationality Assumption from Law and Economics' (2000) 88(4) California Law Rieview 1051.

H. Kunreuther and G. Heal, 'Interdependent security' (2003) 26(2-3) Journal of Risk and Uncertainty 231.

H. Kunreuther, R. Hogarth and J. Meszaros, 'Insurer ambiguity and market failure' (1993) 7(1) Journal of Risk and Uncertainty 71.

Rob van de Laar, 'Cyberrisico's: Meer dan ICT' (2013) 10 AMplus 49.

William M. Landes and Richard A. Posner, *The Economic Structure of Tort Law* (Harvard University Press 1987).

S. Laube and R. Böhme, 'The Economics of Mandatory Security Breach Reporting to Authorities' (Thirtheenth Annual Workshop on the Economics of Information Security, Pennsylvania, 2014).

W. Lee and J.A. Ligon, 'Moral Hazard in Risk Pooling Arrangements' (2001) 68(1) Journal of Risk and Insurance 175.

K. de Leeuw & J. Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007).

T.M. Lenard and P.H. Rubin, 'Much Ado About Notification' (Regulation 44, 2006).

P. Luzwick, 'If Most of Your Revenue is From E-commerce, Then Cyber-Insurance Makes Sense' (2001) 2001(3) Computer Fraud and Security 16.

Ruperto P. Majuca, William Yurcik and Jay P. Keasan, 'The Evolution of Cyberinsurance' (Arxiv 2006) <http://arxiv.org/abs/cs/0601020> accessed 21 March 2016.

Marsh & McLennan Companies, '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 30 March 2018.

J.M. Marshall, 'Insurance Theory: Reserves Versus Mutuality' (1974) Economic Inquiry 476.

Karl Marx and Friedrich Engels, *The Communist Manifesto* (London 1848).

McKinsey & Company, 'McKinsey on Finance' (2012) <http://www.mckinsey.com/client_service/corporate_finance/latest_thinking/~/media/D2CF206B82C34F1FBB87FE591599A958.ashx> accessed 30 March 2018.

A. Meeuwese and M. Versteeg, 'Quantitative Methods for Comparative Constitutional Law' in M. Adams and J. Bonhoff (eds), *Practice and Theory in Comparative Law* (Cambridge University Press 2012).

D. Le Métayer and S. Monteleone. 'Automated consent through privacy agents: Legal requirements and technical architecture' (2009) 25(2) Computer Law & Security Review 136.

Tyler Moore, 'The Economics of Cybersecurity: Principles and Policy Options' (2010) 3(3-4) International Journal of Critical Infrastructure Protection 103.

Tyler Moore, Richard Clayton and Ross Anderson, 'The Economics of Online Crime' (2009) 43(3) Journal of Economic Perspectives 3.

Arunhaba Mukhopadhyay, Samir Chatterjee, Debashis Saha, Ambuj Mahanti and Samir K. Sadhukhan, 'Cyber-Risk Decision Models: To Insure IT or not?' (2013) 56(1) Decision Support Systems 11.

D.K. Mulligan, 'Security Breach Notification Laws: Views from Chief Security Officers' (Berkeley School of Law, 2007) <https://www.law.berkeley.edu/files/cso_study.pdf> accessed 30 March 2018.

D.K. Mulligan and F.B. Schneider, 'Doctrine for Cybersecurity' (2011) 140(4) Daedalus 70.

Anna Nagurney and Shivani Shukla, 'Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability' (2017) 260(2) European Journal of Operational Research 588.

NAIC, 'Cyber Risk' (2013) <http://www.naic.org/cipr_topics/topic_cyber_risk.htm> accessed 30 March 2018.

Nederlandse Vereniging van Banken, 'Fraude' (*NVB* 30 August 2017) <https://www.nvb.nl/thema-s/veiligheid-fraude/586/fraude.html> accessed 30 March 2018.

Nederlandse Vereniging van Banken, 'Hoe hoog is de schade door fraude met Internetbankieren?' (*NVB* 30 August 2017) <https://www.nvb.nl/veelgestelde-vragen/veiligheid-fraude/1816/hoe-hoog-is-de-schade-door-fraude-met-Internetbankieren.html> accessed 30 March 2018.

Bernold F.H. Nieuwesteeg, *The Legal Position and Societal Effects of Security Breach Notification Laws* (Delex 2014).

Bernold Nieuwesteeg, 'Quantifying Key Characteristics of 71 Data Protection Laws' (2016) 7 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 182.

Bernold Nieuwesteeg, 'The Law and Economics of Risk Pooling Arrangements in Cyber Security: the Case of Dutch Higher Education Institutions' (Working Paper presented at the 2017 Seminar on the Future of Law and Economics, 24 March 2017).

Bernold Nieuwesteeg and Michael Faure, 'Data Breach Notification Laws: carrots, sticks and thresholds' (Working Paper presented at the 34th Annual Conference of the European Association of Law and Economics (EALE), the 13th Annual Conference of the Italian Association of Law and Economics (SIDE), the 17th Annual Workshop on the Economics of Information Security (WEIS), 14 September 2017, 15-16 December 2017 and 18-19 June 2018 respectively).

Bernold Nieuwesteeg, Louis Visscher & Bob de Waard 'The Law and Economics of Cyber Insurance Contracts – A Case Study (2018) European Review of Private Law (forthcoming).

Bernold Nieuwesteeg, Louis Visscher & Bob de Waard 'De rechtseconomie van cyberverzekeringen' (2017) 3 Het Verzekerings-Archief 155.

Bernold F.H. Nieuwesteeg, Louis T. Visscher and Bob R.J. De Waard, 'The Law and Economics of Cyber Insurance Contracts – A Case Study' (2016) Working Paper, LDE Centre for Safety and Security, Rotterdam, the Netherlands <http://www.safety-and-security.nl/uploads/cfsas/attachments/The%20Law%20%26%20Econo

mics%20of%20Cyber%20Insurance%20Contracts%20-%20A%20Case%20Study.pdf> accessed 30 March 2018.

Sharon Oded, 'Inducing corporate compliance: A compound corporate liability regime' (2011) 31(4) International Review of Law and Economics.

Sharon Oded, 'Inducing Corporate Proactive Compliance: liability control & corporate monitors' (Diss, Erasmus School of Law 2012).

Hulisi Öğüt, Srinivasan Raghunathan and Nirup M. Menon, 'Information Security Risk Management through Self-Protection and Insurance' (University of Texas, 2005).

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'(2011) 31(3) Risk Analysis 497.

Pramod Pandya, 'Local Area Network Security'in John R. Vacca (ed), *Network and System Security* (2nd edn, Syngress 2014).

Massimiliano Pappalardo, 'Personal data or non-personal data, that is the question! The different interpretations of ECJ and Italian Supreme Court' (Lexology 25 October 2016) <https://www.lexology.com/library/detail.aspx?g=804ce9b8-dfa5-4c67-bbf7-4cc3e087c2f8> accessed 30 March 2018.

Francesco Parisi, 'Positive, Normative and Functional Schools in Law and Economics' (2004) 18 Eur. J. L. Econ. 259.

Francesco Parisi, *The Language of Law and Economics* (Cambridge University Press 2013).

Francesco Parisi and Jonathan Klick, 'Functional Law and Economics: The Search for Value-Neutral Principles of Lawmaking' (2004) Faculty Scholarship Paper 1131. <http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2131&context=faculty_scholarship> accessed 30 March 2018.

Mark V. Pauly, 'The Economics of Moral Hazard: Comment' (1968) 58(3) American Economic Review 531.
Maryant Fernández Pérez, 'Data protection and privacy must be excluded from TTIP' (EDRi 2015).

C. Pfleeger, 'Data security' in: A. Ralston, E.D. Reilly & D. Hemmendinger (eds), *Encyclopedia of Computer Science* (4th edn, Wiley 2003).

PGI Cyber, 'SMEs are Vulnerable to Cyber Attacks' (2015) < http://www.pgitl.com/explore/article/smes-are-vulnerable-to-cyber-attacks> accessed 30 March 2018.

A.M. Polinsky, 'Strict Liability Versus Negligence in a Market Setting' (1980) American Economic Review 363.

A.M. Polinsky and S. Shavell, 'The Theory of Public Enforcement of Law' (2005) Harvard Law School John M. Olin Center for Law, Economics and Business Discussion Paper Series. Paper 529.

A.M. Polinsky and S. Shavell, 'Mandatory versus Voluntary Disclosure of Product Risks' (2006) Harvard Law School John M. Olin

Center for Law, Economics and Business Discussion Paper Series. Paper 564.

Eric A. Posner, *Law and Social Norms* (Harvard University Press 2000).

Richard A. Posner, 'A Theory of Negligence' (1972) 1 Journal of Legal Studies 29.

Richard A. Posner, *Economic Analysis of Law* (Aspen Publishers 1998).

Richard A. Posner, *The Economics of Public Law* (Edward Elgar Publishing, 2001).

Richard A. Posner, 'The Law and Economics Movement: From Bentham to Becker', in F. Parisi and C.K. Rowley (eds) *The Origins of Law and Economics: Essays by the Founding Fathers* (Edward Elgar Publishing 2005).

Richard A. Posner, *Economic Analysis of Law* (Wolters Kluwer Law and Business 2007).

Benjamin Powell, 'Is Cybersecurity a Public Good? Evidence from the Financial Services Industry' (2001) Independent Institute Working Paper Number 57 <http://www.independent.org/pdf/working_papers/57_cyber.pdf> accessed 30 March 2018.

G.L. Priest, 'The Current Insurance Crisis and Modern Tort Law' (1987) Yale Law Journal 1521.

Privacy International, 'National Privacy Ranking' (2007).

Privacy International, 'European Privacy and Human Rights 2010' (2010).

Philip Rawlings, 'Cyber Risk: Insuring the Digital Age' (2015) Queen Mary School of Law Legal Studies, Research Paper 189.

A. Renda, *Law and Economics in the Ria Wold* (Intersentia 2011).

Robert F. Rich, 'The Pursuit of Knowledge' (1979) Knowledge: Creation, Diffusion and Utilization 6.

Markus Riek, Rainer Böhme, Michael Ciere, Carlos Ganan and Michel van Eeten, 'Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries' (2016) Working Paper TU Delft <http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_54-2.pdf> accessed 30 March 2018.

Markus Riek, Rainer Böhme and Tyler Moore, 'Understanding the influence of cybercrime risk on the e-service adoption of European Internet users.' (13th Annual Workshop on Economics of Information Security, Pennsylvania State University, 2014) <http://www.econinfosec.org/archive/weis2014/papers/RiekBoehmeMoore-WEIS2014.pdf> accessed 30 March 2018.

Everett M. Rogers, *Diffusion of Innovation* (5th edn, Simon & Schuster 2003).

S. Romanosky, Hoffman and A. Acquisti, 'Empirical Analysis of Data Breach Litigation'(2014) 11(1) Journal of Empirical Legal Studies 74.

S. Romanosky, R. Telang and A. Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) Journal of Policy Analysis and Management 256.

N.J. Ronneberg, 'An Introduction to the Protection & Indemnity Clubs and the Marine Insurance They Provide' (1990) 25 University of San Francisco Maritime Law Journal 1.

P. Rosati, M. Cummings, P. Deeney, F. Gogolin, L. van der Werff and T. Lynn, 'The effect of data breach announcements beyond the stock price: Empirical evidence on market activity' (2017) 49 International Review of Financial Analysis 146.

Michael Rothschild and Joseph Stiglitz, 'Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information' (1976) 90(4) The Quarterly Journal of Economics 629.

Jean-Jacques Rousseau, *Du Contract Social* (Amsterdam: Marc-Michel Rey 1762).

B.R. Rowe and M.P. Gallaher, 'Private Sector Cyber Security Investment Strategies: An Empirical Analysis' (Fifth Annual Workshop on the Economics of Information Security, Cambridge, 2006) <http://www.econinfosec.org/archive/weis2006/docs/18.pdf> accessed 30 March 2018.

David Rowell and Luke B. Connelly, 'A History of the Term "Moral Hazard"' (2012) 79(4) Journal of Risk and Insurance 7

Jorge Sábato and M. Mackenzi, *La producción de technologia. Autónoma o transnacional* (Nueva Imagen 1982).

C.W. Sanchirico, 'Deconstructing the New Efficiency Rationale' (2001) 86(6) Cornell Law Review 1003.

Hans-Bernd Schäfer and Claus Ott, *The Economic Analysis of Civil Law* (Edward Elgar Publishing 2005).

Stuart E. Schechter and Michael D. Smith, 'How Much Security Is Enough to Stop a Thief?' (International Conference on Financial Cryptography, Guadeloupe, January 2003).

Fabian A. Scherschel, 'Petya, Mischa, Goldeneye: Die Erpresser sind Nerds' *Heise Online* (15 December 2016) <https://www.heise.de/newsticker/meldung/Petya-Mischa-Goldeneye-Die-Erpresser-sind-Nerds-3571937.html> accessed 30 March 2018.

Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (Springer, 2003).

Bruce Schneier, 'State Data Breach Notification Laws: Have They Helped?' (2009) Information Security.

Bruce Schneier, 'Feudel Security' (*Schneier,* 3 December 2012) <https://www.schneier.com/blog/archives/2012/12/feudal_sec.html> accessed 30 March 2018.

Daniel Schwarcz and Peter Siegelman (eds), *Research Handbook on the Economics of Insurance Law* (Edward Elgar Publishing 2015).

Paul M. Schwartz, 'Internet Privacy and the State' (1999) 32 Connecticut Law Review 815.

Paul M. Schwartz and Edward J. Janger. 'Notification of Data Security Breaches' (2007) 105(5) Michigan Law Review 913.

Menno Sedee, 'Cyberaanval-blog: ook tweede terminal APM in Rotterdam deels open' (NRC) <https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693> accessed 30 March 2018.

Andreea M. Serban and Jing Luan, 'Overview of Knowledge Management' (2002) 2002(113) New Directions for Institutional Research 5.

Scott J. Shackelford, 'Should Your Firm Invest in Cyber Risk Insurance?' (2012) 55(4) Business Horizons 349.

S. Shavell, 'On Moral Hazard and Insurance' (1979) 93 Quarterly Journal of Economics 541.

S. Shavell, *Economic Analysis of Accident Law* (Harvard University Press 1987).

S. Shavell, *Foundations of Economic Analysis of Law* (Harvard University Press 2004).

Nikhil Shetty, Galina Schwartz, Mark Felegyhazi and Jean Walrand, 'Competitive Cyber-Insurance and Internet Security' in T. Moore, D.

Pym, and C. Ioannidis (eds), *Economics of Information Security and Privacy* (New York: Springer 2010).

Goran Skogh, 'The Transactions Cost Theory of Insurance: Contracting Impediments and Costs' (1989) 56(4) The Journal of Risk and Insurance 726.

Goran Skogh, 'Insurance and the Institutional Economics of Financial Intermediation' (1991) 16 The Geneva Papers on Risk and Insurance 360.

Goran Skogh, 'Development Risks, Strict Liability, and the Insurability of Industrial Hazards' (1998) 23 The Geneva Papers on Risk and Insurance 247.

Goran Skogh, 'Risk-sharing institutions for unpredictable losses' (1999) 155 Journal of Institutional and Theoretical Economics 505.

Goran Skogh, 'Risk-sharing and insurance: contracts with different institutional implications', in T. Eger, J. Bigus, C. Ott and G. Van Wangenheim (eds), *Internationalisation of the law and its economic analysis Festschrift für Hans-Bernd Schäfer zum 65. Geburtstag* (Wiesbaden: Gabler Editions 2008).

G. Skogh and H. Wu, 'The diversification theorem restated: risk pooling without assignment of probabilities' (2005) 31(1) The Journal of Risk and Uncertainty 35.

F. Skopik, G. Settanni and R. Fiedler, 'A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through information sharing' (2016) 60 Computers & Security 154.

Nader S. Safa and R. Von Solms, 'An information security knowledge sharing model in organizations' (2016) 57 Computers in Human Behavior 442.

James Stevenson and Richard J. Prevost, 'Securing the Grid: Information Sharing in the Fifth Dimension' 2013 26(9) The Electricity Journal 42.

G.J. Stigler, 'The Optimum Enforcement of Laws' (1970) 78(3) Journal of Political Economy 526.

G.J. Stigler, *The Optimum Enforcement of Laws* (NBER 1974) ch, 55.

Joseph E. Stiglitz, 'Markets, Market Failures, and Development' (1989) 79(2) American Economic Review 197.

Øivind Strand and Loet Leydesdorff, 'Where is synergy indicated in the Norwegion innovation system? Triple-Helix relations among technology, organization, and geograpy'(2013) 80(3) Technological Forecasting and Social Change 471.

Husam Suleiman, Algassem Israa, Ali Diabat, Edin Arnautovic and Devor Svetinovic, 'Integrated Smart Grid Systems Security Threat Model' (2015) 53(C) Journal of Information Systems 147.

Symantec, '2017 Internet Security Threat Report' (2017) <https://www.symantec.com/security-center/threat-report> accessed 30 March 2018.

S. Tajalizadehkhoob, Hadi Asghari, Carlos Ganán and Michel van Eeten, 'Why Them? Extracting Intelligence about Target Selection from Banking Trojans' (13th Annual Workshop on the Economics of Information Security, Pennsylvania State University, 2014) <http://www.econinfosec.org/archive/weis2014/papers/Tajalizadehkhoob-WEIS2014.pdf> accessed 30 March 2018.

Gordon Tullock and Richard McKenzie, *The New World Economics* (4th edn, Richard D. Irwin Publishing 1985).

UNODC, 'Comprehensive Study on Cybercrime' (2013).

Irena Vaivode, 'Triple Helix Model of University-Industry-Government Cooperation in the Context of Uncertainties' (2015) 212 Procedia- Social and Behavioral Sciences 1063.

Hal R. Varian, Joseph Farrell and Carl Shapiro, *The Economics of Information Technology: An Introduction* (Cambridge University Press 2004).

Hal R. Varian, *Intermediate Microeconomics: A Modern Approach* (8th edn, W.W. Norton & Company 2010).

Jennifer R. Veltsos, 'An Analysis of Data Breach Notifications as Negative News' (2012) 75(2) Business Communication Quarterly 192.

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 30 March 2018.

Verbond van Verzekeraars, 'Dutch Insurance Industry in Figures' (2014) <https://www.verzekeraars.nl/media/3635/verzekerd-van-cijfers-2014-en.pdf > accessed 30 March 2018.

Verizon, '2017 Data Breach Investigations Report' (2017) <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/> accessed 30 March 2018.

Etienne Verschuren, 'Wereldwijde aanval met ransomware treft ook deel Rotterdamse haven en TNT' NRC (Amsterdam, 27 June 2017) <https://www.nrc.nl/nieuws/2017/06/27/aanval-met-ransomware-op-containerbedrijf-haven-rotterdam-a1564693> accessed 30 March 2018.

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 2007).

Gerhard Wagner, 'Tort Law and Liability Insurance' in Michael G. Faure (ed), *Tort Law and Economics Volume I Encyclopedia of Law and Economics* (2nd edn, Cheltenham: Edward Elgar 2009).

Alan Watson, *Legal Transplants: An Approach to Comparative Law* (University of Georgia Press 1974).

M. Watt, *Globalization and comparative law* (Oxford University Press, 2006).

E.A. Whitley. 'Informational privacy, consent and the "control" of personal data' (2009) 14(3) Information Security Technical Report 154.

Wikipedia, 'Broodfonds' (21 January 2017) <https://en.wikipedia.org/wiki/Broodfonds> accessed 30 March 2018.

Willis, 'Willis Fortune 1000 Cyber Disclosure Report' (2013) <http://blog.willis.com/downloads/cyber-disclosure-fortune-1000/> accessed 30 March 2018.

J.K. Winn, 'Are "Better" Security Breach Notification Laws Possible?' (2009) 24(3) Berkeley Technology Law Journal 1133.

D.A. Wittman, 'Liability for harm or restitution of benefit?' (1984) 13 Journal of Legal Studies 57.

R. Wong, 'Data protection: The future of privacy' (2011) 27(1) Computer Law & Security Review 53.

Tao Wu, Leiting Chen, Xingping Xian and Yuxiao Guo, 'Evolution prediction of multi-scale information diffusion dynamics' (2016) 113 Knowledge-Based Systems 186.

Y. Wu, Tuenyu Lau, David J. Atkin and Carolyn A. Lin, 'A comparative study of online privacy regulations in the U.S. and China' (2011) 35(7) Telecommunications Policy 603.

William Yurcik and David Doss, 'CyberInsurance; A Market Solution to the Internet Security Market Failure' (First Workshop on the Economics of Information Security, Berkeley, 2002) <http://www.cl.cam.ac.uk/~rja14/econws/53.pdf> accessed 30 March 2018.

Z. Zhao, L. Xue and A.B. Whinston, 'Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements' (2013) 30(1) Journal of Management Information Systems 123.

Zi-Ke Zhang, Chuang Liu, Xiu-Xiu Zhan, Xin Lu, Chu-Xu Zhang and Yi-Cheng Zhang, 'Dynamics of information diffusion and its applications on complex networks' (2016) 651 Physics Reports 1.

Peter Zweifel and Roland Eisen, *Versicherungsökonomie* (2nd edn, Springer 2003).

K. Zweigert and H. Kötz, *Introduction to comparative law* (3rd edn, Clarendon Press 1998).

CASES

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECR I-650.

Case C-131/12 *Google Spain SL, Google Inc. V Agencia Espa Española de Protección de Datos* [2014] ECR I-317.

Travelers Indemnity Co. of America v. *Portal Healthcare Solutions LLC* 14-1944 U.S. Court of Appeals for the Fourth Circuit.

Recall Total Information Management Inc. et al. v. *Federal Insurance Co. et al.* SC19291 Connecticut Supreme Court.

Travelers Property Casualty Company of America et al. v. *Federal Recovery Services et al.* 2:14-cv-00170 U.S. District Court for the District of Utah.

Interviews

Interview with Mr. Bram Eidhof (Amsterdam, 13 September 2013).

Interview with Mr. Michel van Eeten (Delft, 17 September 2013).

Interview with Ms. Anna Gerbrandy (Utrecht, 30 October 2013).

Interview with Ms. Anne Meuwese (Tilburg, 5 November 2013).

Interview with Ms. Marloes van Rijnsbergen (Utrecht, 27 February 2014).

Interview with Mr. Andrea Renda (Rotterdam, 21 March 2014).

Interview with Mr. Bauke Steenhuizen (Delft, 24 March 2014).

Interview with Ms. Dina Hadziosmanovic (Delft, 3 April 2014).

Interview with Mr. Wolter Pieters (Delft, 3 April 2014).

Interview with Ms. Nady Purtova (Tilburg, 6 April 2014).

Interview with Mr. John Klick (Rotterdam, 14 April 2014).

Interview with Mr. Rommert Dekker (Rotterdam, 14 April 2014).

Interview with Ms. Rina Steenkamp (The Hague, 17 April 2014).

Interview with Ms. Marga Groothuis (The Hague, 23 April 2014).

Interview with Mr. Kas Clark (The Hague, 30 April 2014).

Interview with Mr. Ton Siedsma (Amsterdam, 1 May 2014).

Interview with Mr. Fabio Bisogni (Rotterdam, 8 May 2014).

Interview with Mr. Bart Pegge (Rotterdam, 21 May 2014).

Interview with Ms. Anne Wil Duthler (The Hague, 2 June 2014).

Interview with Ms. Tatiana Tropina (Rotterdam, 2 June 2014).

Interview with Mr. Frank Fransen and Mr. Andre Smulders (Delft, 12 June 2014).

Interview with Mr. Andre Hoogstrate (Rotterdam, 9 July 2014).

Interview with Mr. Evert Jan Hummelen and Jeroen Morrien (The Hague, 16 July 2014).

Interview with Mr. Richard van Schaik (Amsterdam, 21 July 2014).

Interview with Mr. Sharon Oded (Rotterdam, 14 August 2014).

Interview with Mr. Maarten van Wieren (Amstelveen, 23 September 2014).

Interview with Mr. Joppe Willeboordse (Bologna, 3 October 2014).

Interview with Mr. Mark Buning (Bologna, 10 October 2014).

Interview with Mr. Jos Schaffers (Rotterdam, 13 April 2015).

Interview with Ms. Mila Versteeg (Hamburg, 5 June 2015).

Interview with Mr. Genserik Reniers (Delft, 15 December 2015).

Interview with Ms. Biba Schoenmaker (Rotterdam, 11 February 2016).

Interview with Mr. Rob van den Hoven van Genderen (Amsterdam, 15 March 2016).

Interview with Ms. Lokke Moerel (Amsterdam, 22 March 2016).

Interview with Mr. Roel Wieringa (Rotterdam, 13 April 2016).

Interview with Mr. Bert Feskens (Amsterdam, 25 May 2016).

Interview with Mr. Rainer Böhme (Rotterdam, 16 June 2016).

Interview with Mr. Melle van den Berg (Rotterdam, 20 July 2016).

Interview with Mr. Frank Koppejan (Amsterdam, 23 August 2016).

Interview with Mr. Max Smeets (Amsterdam, 15 September 2016).

Interview with Mr. Rick Hofstede (The Hague, 21 October 2016).

Interview with Mr. Dennis Broeders (Rotterdam, 2 March 2017).

Interview with Mr. Steffen Morrees (Amsterdam, 9 May 2017).

Interview with Ms. Renée Visser (Amsterdam, 6 June 2017).

Interview with Ms. Elly van den Heuvel (The Hague, 6 July 2017)

Interview with Ms. Corien Prins (The Hague, 11 July 2017).

SUMMARY

Over the last decade an increasing amount of cyber attacks threatened the functioning of the global economy. It is hard for organizations to determine their 'optimal' level of security. In order to attain this, this study advocates that information related to the nature of cyber risk and the return on investment of measures to reduce it diffuses among relevant actors, while taking into consideration the costs of doing so. Currently, there is insufficient information diffusion in cyber security. This study seeks to identify solutions for the efficient stimulation of cyber security information diffusion. The strong public good characteristics of information diffusion - the diffuser of information has little benefits from diffusing it - complicate this endeavour.

In order to fulfil this promise, *law and economics* must gain a deeper link with the *economics of cyber security*. Scholars in the economics of cyber security should benefit from the development of theory and methodology within law and economics. Scholars in law and economics should learn from the insights regarding the dynamics, empirics and microeconomic peculiarities of cyber risk as encountered in the economics of cyber security. Significant efforts to link the fields are required, because there is a large gap to be bridged.

This *law and economics of cyber security* has taken up the task to further formulate a common 'cyber security information diffusion' agenda for university, government and industry. Each party within this 'triple helix' has different roles, responsibilities and tools to stimulate information diffusion. The deployment of the individual tools available to these three parties combined with their mutual cooperation will yield the most fruitful results. This study made a first step in doing so in its three substantive parts.

Part I epitomizes the role of university and presents a pioneering analysis that unlocks six characteristics in the text of 71 DPLs. It diffuses information about concepts within a number of DPLs and discloses them for statistical analysis, which is beneficial to the connection of law and economics with the economics of cyber security because the latter field has empirical data that in such a way can be connected to the effects of legislation. Hereafter, Part II exemplifies the role of government and studies the EU DBNL embedded in the GDPR. The study reveals that the EU DBNL could incentivize organizations to stimulate information diffusion, provided that it will be enforced wisely by the national data protection authorities. I urge the data protection authorities to look at tailor made carrots and the expressive function of the law as alternative incentive schemes. Also, the threshold for notifying individuals needs to be fairly high and clear-cut. Last, Part III focuses on industry, more specifically cyber risk insurance and pooling, which is risk shifting without the interference of an insurer. The empirical analysis on cyber insurance shows that the market for small- and medium enterprises is still in its infancy and that information diffusion between the insurer and insured is limited. Cyber risk pooling could play an important role in situations where organizations have more or equal information about cyber risk compared to insurers. Cyber risk pooling can potentially move organizations to desirable (hybrid) forms of risk allocation where also individual management and cyber insurance play a role. The analysis sketches which specific conditions and design issues have to be taken into account regarding pooling.

The further integration of our analogue lives with the digital world will inevitably continue. So will its downsides, in the near and distant future. The law and economics of cyber security can provide a

foundation that enables further prosperity and empowerment in the digital era.

SAMENVATTING

Een toenemend aantal cyberaanvallen bedreigde het afgelopen decennium de wereldeconomie. Voor organisaties is het lastig om een optimaal niveau van veiligheid te bepalen. Om dit te verbeteren, bepleit deze studie dat het noodzakelijk is om de informatie over de aard van het cyberrisico en het rendement van de investering in maatregelen om het risico te verminderen te delen onder relevante actoren, waarbij men de kosten van deze kennisdeling in acht neemt. Op dit moment is er onvoldoende kennisdeling in cybersecurity. Daarom zoekt deze studie oplossingen voor efficiënte stimulering van kennisdeling in cybersecurity. Kennisdeling heeft sterke trekken van een publiek goed: degene die de informatie deelt, heeft er zelf weinig baat bij. Dit bemoeilijkt deze uitdaging.

Allereerst moet de rechtseconomie beter verbonden worden met de economie van cybersecurity. Onderzoekers in de economie van cybersecurity zouden gebruik moeten maken van de theoretische en methodologische kennis uit de rechtseconomie. En onderzoekers in de rechtseconomie zouden moeten leren van de inzichten met betrekking tot de dynamiek, empirie en specifieke micro-economische aspecten van de economie van cybersecurity. We moeten een flinke inspanning doen om de twee gebieden bij elkaar te brengen.

Deze *rechtseconomie van cybersecurity* moet de taak op zich nemen om een gemeenschappelijke 'cybersecurity kennisdelingsagenda' te definiëren voor zowel wetenschap als overheid en bedrijfsleven. Elke partij in deze 'triple helix' heeft verschillende rollen, verantwoordelijkheden en middelen om kennisdeling te stimuleren. De ontwikkeling van die individuele middelen, gecombineerd met intensieve samenwerking, zal de beste resultaten opleveren. Deze

studie heeft in de drie inhoudelijke delen een eerste stap in deze richting gezet.

Deel 1 richt zich op de rol van de wetenschap zelf en presenteert een pionierende analyse die zes aspecten in de wettekst van 71 persoonsgegevensbeschermingswetten ontsluit. Het deel deelt informatie met betrekking tot concepten binnen deze wetten en maakt ze gereed voor statistische analyse, wat de verbinding tussen rechtseconomie en de economie van cybersecurity ten goede komt. De laatste heeft namelijk veel empirische data die op deze manier verbonden kunnen worden met de effecten van wetgeving. Hierna richt Deel 2 zich op de rol van de overheid en bestudeert de nieuwe Europese meldplicht datalekken, verankerd in de Europese Algemene Verordening Gegevensbescherming. De studie openbaart dat deze Europese meldplicht prikkels kan geven om organisaties te stimuleren om informatie te delen, maar alleen als deze slim gehandhaafd wordt door de nationale autoriteiten. Ik spoor deze autoriteiten dan ook aan om slimme beloningen te ontwerpen en ook te kijken naar de expressieve functie van de wet als alternatieve manieren om de juiste prikkels te geven aan de organisaties die de wet moeten naleven. Een laatste punt is dat de drempel om te melden relatief hoog moet zijn en in ieder geval duidelijk. Als laatste focust Deel 3 op de rol van de industrie, en in het bijzonder onderzoekt dit deel cyberverzekeringen en cyberriskpooling (risicoverschuiving zonder tussenkomst van een verzekeraar). De empirische analyse van cyberverzekering laat zien dat de markt voor het midden- en kleinbedrijf nog in de kinderschoenen staat en dat de kennisdeling tussen de verzekeraar en de verzekerde nog zeer beperkt is. Cyberriskpooling kan een belangrijke rol spelen in situaties waarin organisaties meer (of gelijke) informatie over het cyberrisico hebben dan de verzekeraar. Met cyberriskpooling kunnen organisaties een gewenste hybride vorm van

risicoallocatie kiezen, waarin ook cyberverzekeringen en eigen beheer van het risico een rol spelen. De analyse schetst welke voorwaarden en ontwerpvragen bij cyberriskpooling in acht moeten worden genomen.

De verdere verbondenheid van onze analoge levens met de digitale wereld zal zich onvermijdelijk voortzetten. Zo ook de nadelen hiervan, in de nabije en verre toekomst. De rechtseconomie van cybersecurity kan deze ontwikkeling van een fundament voorzien waardoor we verdere welvaart- en welzijnsgroei in het digitale tijdperk kunnen realiseren.

EDLE PhD Portfolio

PhD-period: March 2014 – February 2018

PhD training	
Bologna courses	***year***
Introduction into the Italian legal system	2014
Statistics	2014
Economics analysis of law	2014
Game theory	2014
Experimental law and economics	2014
Game theory and the law	2014
European securities and company law	2015
Behavioral law and economics and enforcement mechanisms	2015
Specific courses	***year***
Seminar 'How to write a PhD'	2014
Seminar Series 'Empirical Legal Studies'	2014
Networkshop IVIR	2014
Academic Writing Skills for PhD students (Rotterdam)	2015
Course presentation skills (Rotterdam)	2017
Seminars and workshops	***year***
Bologna November seminar (attendance)	2014
Rotterdam Fall seminar series (peer feedback)	2015
Rotterdam Winter seminar series (peer feedback)	2016
Joint Seminar 'The Future of Law and Economics' (attendance)	2016
Presentations	***year***
Colloquium Econsec TU-Delft	2014
Dispuut Oud Kruisinga	2014
NCSRA Symposium	2014
Dispuut Oud Kruisinga	2014
Bologna March seminar	2015
Hamburg June seminar	2015
Rotterdam Fall seminar series	2015
Rotterdam Winter seminar series	2016
BNR Nieuwsradio	2016

Open Minded Leiden	2016
Colloquium Econsec TU-Delft	2016
Pitch cybersecurity seaside matchmaking event	2016
Bologna November seminar	2016
LDE centre for safety and security key note Delft	2017
Cyber risk pooling Wageningen	2017
Joint Seminar 'The Future of Law and Economics'	2017
Attendance (international) conferences	***year***
Symposium Internet & Recht Amsterdam	2014
EALE 2014 Aix en Provence	2014
CPDP 2014 Brussels	2015
WEIS 2015 Delft	2015
NILG conference 2015 Amsterdam	2015
SIDE 2015 Naples	2015
SIDE 2016 Turin	2016
CRESSE 2017 Heraklion	2017
EALE 2017 London	2017
SIDE 2017 Rome	2017
WEIS 2018 Innsbruck	2018
Teaching	***year***
Economics of Privacy (Erasmus University)	2015
Economics of Cyber Security (Erasmus University)	2015
Economics of Privacy (minor Recht & Techniek Delft)	2017

Curriculum Vitae – Bernold Nieuwesteeg

Personal Details

Name:	B.F.H. (Bernold) Nieuwesteeg
Email:	nieuwesteeg@law.eur.nl
Nationality:	Dutch

Short bio

Bernold Nieuwesteeg is a Law and Economics researcher at Rotterdam Institute of Law and Economics (RILE), Erasmus University Rotterdam, The Netherlands. Bernold has been a Ph.D. researcher in the European Doctorate in Law and Economics (EDLE) Program. Bernold is partner at CrossOver, and advised leading firms in the energy- and utility sector.

Work experience

2014 – now	**PhD candidate in the law and economics of cyber security** PhD candidate at the European Doctorate of Law & Economics (Erasmus University Rotterdam, University of Hamburg and University of Bologna).
2013 - now	**Partner at CrossOver** CrossOver offers programs for joint development and knowledge sharing between people of different organizations.
2011 - 2014	**Founder at InvestMens** InvestMens is a concept for a social investment fund in human capital with founding partners Randstad, PGGM, and three Dutch ministries.

2012 – 2013	**Project leader at Ruim Baan** Analyzing and proposing solutions to overcome the upcoming shortage of technical employees at Dutch utility companies.
2011	**Participant at the Dutch National Think Tank** Analyzing the future of the Dutch labour market, together with 21 other young academics. Trained by, amongst others, McKinsey & Company.

Publications (selection)

2018	Nieuwesteeg, B.F.H., Visscher, L.T., de Waard B.J.R. *The Law and Economics of Cyber Insurance Contracts: A Case Study.* European Review of Private Law.
2018	Nieuwesteeg, B.F.H., *Ineffectiviteit 'sleepwet' is laatste strohalm voor de tegenstanders.* Financieel Dagblad.
2018	Nieuwesteeg, B.F.H., *Meldplicht datalek kan ook tot publieke onverschilligheid leiden.* Financieel Dagblad.
2018	Faure, M.G., Nieuwesteeg, B.F.H. *Cyber Risk Pooling.* NYU Journal of Law and Business (forthcoming).
2017	Nieuwesteeg, B.F.H., *Alle hacks voorkomen? Niet tegen elke prijs.* NRC-Handelsblad.
2017	Nieuwesteeg, B.F.H., *Book Review.* Common Market Law Review.
2017	Nieuwesteeg, B.F.H., Visscher, L.T., de Waard B.J.R. *De rechtseconomie van cyberverzekeringen.* Het Verzekerings-archief.
2016	Nieuwesteeg, B.F.H. *De invoering van de meldplicht datalekken*. Aansprakelijkheid, verzekering en schade.

2016	Nieuwesteeg, B.F.H. *Quantifying Key Characteristics of 71 Data Protection Laws.* Journal of Intellectual Property, Information Technology and E-Commerce Law.
2014	Nieuwesteeg, B.F.H. *The Legal Position and Societal Effects of Security Breach Notification Laws.* Amsterdam: Delex.
2013	Eidhof, B.B.F., Nieuwesteeg, B.F.H. *Haalbaarheidsstudie InvestMens.* The Hague: Ministry of Social Affairs.

Education

2008 - 2013	**Utrecht University** Master European Law (Cum Laude) Bachelor Utrecht Law College (honours program)
2007 - 2013	**Delft University of Technology** Master Systems Engineering, Policy Analysis and Management Bachelor Technische Bestuurskunde
2001 - 2007	**Christelijk Gymnasium Utrecht**

Other professional activities

2012 - now	**Treasurer at the InvestMens foundation** The InvestMens foundation aims to increase intersectoral job-to-job mobility.
2012 - 2016	**Member of the board of alumni at the Dutch National Think Tank** Utilizing the potential of our network through the facilitation of initiatives from and activities for the alumni.
2011 - 2012	**Founder, producer and actor at Bureau Klein Leed**

BKL is a semi-professional and financially independent theatre group. Learn more at bureaukleinleed.nl (in Dutch).

2010 - 2011 **President of the Utrecht University Model United Nations**
Presiding the board. Delegate at the Cambridge and Harvard Model United Nations.