

the **LAW** *and*
ECONOMICS *of*
CYBER SECURITY



BERNOLD NIEUWESTEEG

The Law and Economics of Cyber Security



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



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

© 2018 B.F.H. Nieuwesteeg

ISBN: 978-90-8692-069-3

NUR: 820

Uitgeverij deLex

www.deLex.nl

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.



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA



Universität Hamburg



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 Bronsvort, 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 (broederschap), 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

Table of Contents.....	xiii
Detailed Table of Contents	xv
SETTING THE STAGE: THE CYBER SECURITY THEATRE.....	1
1. INTRODUCTION	3
2. INFORMATION DIFFUSION AND THE TRIPLE HELIX	53
PART I:.....	83
3. QUANTIFYING KEY CHARACTERISTICS OF 71 DATA PROTECTION LAWS	85
PART II:.....	133
4. DATA BREACH NOTIFICATION LAWS: CARROTS, STICKS AND THRESHOLDS.....	135
PART III:.....	173
5. INTRODUCTION TO PART III: THE POTENTIAL OF RISK SHIFTING	175
6. CYBER INSURANCE CONTRACTS: A CASE STUDY.....	191
7. CONDITIONS FOR CYBER RISK POOLING.....	247
CONCLUSION	281
8. CONCLUSION AND SYNTHESIS.....	283
BIBLIOGRAPHY	315
SUMMARY.....	357
SAMENVATTING	361

Detailed Table of Contents

Acknowledgements.....	ix
Table of Contents.....	xiii
Detailed Table of Contents	xv
List of Acronyms and Abbreviations.....	xxiii
List of Tables	xxv
List of Figures.....	xxvii
SETTING THE STAGE: THE CYBER SECURITY THEATRE.....	1
1. INTRODUCTION	3
1.1. Introduction.....	3
1.2. The Methodology and Procedural Strategy of the Study	12
1.2.1 Law and economics and economics of cyber security.....	12
1.2.2 The core methodology and paradigm.....	16
1.2.3 Process strategy.....	18
1.3. Investing in Cyber Security.....	20
1.3.1 Cyber risk	20
1.3.2 Threat	21
1.3.3 Vulnerability.....	25
1.3.4 Impact	27
1.3.5 Cyber risk as a systemic risk.....	29
1.3.6 Investing in resilience.....	31
1.3.7 Market power of software and security companies	32
1.4. Cyber Security and Social Welfare	34
1.4.1 The contribution of a social welfare perspective	36
1.4.2 Pricing the social welfare function	37
1.4.3 Other criteria for the distribution of cyber security investments.....	40
1.5. Misaligned Incentives.....	42
1.5.1 Externalities and public good characteristics.....	43
1.5.2 Information deficits	46
1.6. Summary.....	51
2. INFORMATION DIFFUSION AND THE TRIPLE HELIX.....	53

2.1.	Introduction.....	53
2.2.	Information Diffusion.....	54
2.2.1	The information value chain.....	54
2.2.2	The social benefit of information diffusion	57
2.2.3	The social cost of information diffusion	60
2.2.4	The practice of information diffusion	61
2.3.	Focus on Legal Instruments.....	63
2.3.1	Challenges for the utilization of legal instruments in cyber security.....	63
2.3.2	The legal instruments that the study did not include	65
2.4.	A 'Triple Helix' Approach Towards the Specific Issues of the Study	66
2.5.	Information Diffusion and the Triple Helix	70
2.5.1	Part I.....	71
2.5.2	Part II.....	73
2.5.3	Part III	74
2.5.4	Connection between the parts	76
2.6.	Summary.....	78
PART I:		83
3. QUANTIFYING KEY CHARACTERISTICS OF		71
DATA PROTECTION LAWS		85
3.1.	Introduction.....	85
3.2.	Quantitative Text Analysis and DPLs.....	86
3.2.1	QTA facilitates information diffusion about the law	86
3.2.2	QTA unlocks the law for statistical analysis	87
3.2.3	The social benefit of DPLs.....	89
3.2.4	The notion of privacy control	90
3.3.	The Dataset	93
3.3.1	Existing datasets.....	93
3.3.2	The dataset adopted: the DLA Piper data protection handbook	98
3.4.	The Six Coded Characteristics	99

3.4.1	Data collection requirements	101
3.4.2	Data breach notification law	102
3.4.3	Data protection authority (DPA).....	104
3.4.4	Data protection officer (DPO).....	105
3.4.5	Monetary sanctions.....	106
3.4.6	Criminal sanctions	108
3.4.7	Correlations between the individual characteristics	108
3.5.	Identifying Underlying Unobserved Variables	110
3.5.1	Principal component analysis.....	110
3.5.2	Basic and advanced characteristics	110
3.6.	Aggregating Underlying Factors towards a ‘Privacy Control Index’	113
3.6.1	The privacy control index	113
3.6.2	Relation with other indices	115
3.6.3	Explanatory power of the index and the coded characteristics.....	116
3.6.4	Limitations.....	120
3.7.	Concluding Remarks	121
	Appendix A	123
	Appendix A.1. The six characteristics.....	123
	Appendix A.2. The full privacy control index and the two underlying factors.....	125
	Appendix A.3. Long list of characteristics.....	127
	Appendix A.4. Overview of coded characteristics	130
	Appendix A.5. Scree Plot Principal Component Analysis.....	131
	PART II:.....	133
4.	DATA BREACH NOTIFICATION LAWS: CARROTS, STICKS AND THRESHOLDS.....	135
4.1.	Introduction.....	135
4.2.	The European Union Data Breach Notification Regulation	138
4.3.	The Social Benefits and Costs of the DBNL.....	141
4.3.1	The threshold	141

4.3.2	The social benefits.....	143
4.3.3	The social costs.....	145
4.3.4	Social costs versus social benefits.....	146
4.4.	Will there be Spontaneous Disclosure in the Absence of the Law?	147
4.4.1	Private benefits.....	147
4.4.2	Private costs.....	148
4.5.	The Case for the DBNL.....	152
4.5.1	Is there a case for the DBNL?.....	152
4.5.2	Public cost of the DBNL	153
4.6.	Will the EU DBNL Sufficiently Induce Organizations to Notify?.....	154
4.6.1	The administrative fine	154
4.6.2	Enforcement of the fine	156
4.6.3	The digital first aid kit	159
4.6.4	The expressive function of the DBNL.....	163
4.6.5	Summary.....	165
4.7.	Which Disclosure Threshold will Contribute to Social Welfare?.....	165
4.7.1	The disclosure threshold for notification to DPAs	166
4.7.2	The disclosure threshold for notification to individuals..	167
4.7.3	Smart Thresholds	168
4.8.	Concluding Remarks	169
PART III:.....		173
5. INTRODUCTION TO PART III: THE POTENTIAL OF RISK SHIFTING.....		175
5.1.	Introduction.....	175
5.2.	Demand for Risk Shifting.....	176
5.2.1	Reducing risk (risk aversion).....	176
5.2.2	Reducing transaction costs.....	177
5.3.	Three Forms of Risk Allocation.....	178
5.3.1	Individual management.....	178

5.3.2	Cyber insurance	180
5.3.3	Cyber risk pooling	181
5.4.	Social Benefits of Risk Shifting	182
5.4.1	Stimulating information diffusion	182
5.4.2	Internalizing externalities	184
5.5.	The Storyline of Chapter 6 and 7.....	185
6.	CYBER INSURANCE CONTRACTS: A CASE STUDY.....	191
6.1.	Introduction.....	191
6.2.	Impediments to the Insurability of Cyber Risk.....	193
6.2.1	The coverage of systemic cyber risk.....	194
6.2.2	Prices and competitors, the impact of information deficits.....	200
6.2.3	Adverse selection.....	205
6.2.4	Reverse adverse selection.....	210
6.2.5	Moral hazard	212
6.3.	Empirical Strategy.....	215
6.4.	Results and Discussion.....	217
6.4.1	Requesting procedure.....	217
6.4.2	Premiums.....	218
6.4.3	Coverage	220
6.4.4	Caps and deductibles	224
6.4.5	Risk reduction measures	226
6.4.6	Insurers and their strategies.....	227
6.5.	Conclusions and Future Research on Cyber Insurance.....	230
6.5.1	Conclusions	230
6.5.2	Future research on cyber insurance	232
	Appendix B.....	234
	Appendix B.1: Coverage of third party liability per insurer	234
	Appendix B.2: Coverage of first party liability per insurer	236
	Appendix B.3: Details of coverage of third party liability.....	238
	Appendix B.4: Details of coverage of first party liability.....	242
7.	CONDITIONS FOR CYBER RISK POOLING.....	247

7.1.	Introduction.....	247
7.2.	Pooling Relative to Insurance	248
7.2.1	Advantages.....	249
7.2.2	Drawbacks	253
7.3.	Experiences in Other Sectors	256
7.3.1	Broodfondsen	256
7.3.2	P&I clubs.....	257
7.3.3	Pooling offshore related risks	259
7.3.4	Ria de Vigo	261
7.4.	Conditions for Effective Cyber Risk Pooling.....	262
7.4.1	Sufficiently unattractive alternatives	262
7.4.2	Effective mutual monitoring.....	263
7.4.3	Practical possibility to set up a pool.....	265
7.5.	The Design of a Cyber Risk Pool	265
7.5.1	The covered risks	266
7.5.2	Size and type of participants on the pool	269
7.5.3	Rules of entry	272
7.5.4	Contribution of each participant	273
7.5.5	Timing of the contribution.....	275
7.6.	Concluding Remarks	276
	CONCLUSION	281
8.	CONCLUSION AND SYNTHESIS.....	283
8.1.	The Three Parts of the Study.....	289
8.1.1	Part I.....	290
8.1.2	Part II.....	291
8.1.3	Part III	293
8.2.	An Agenda for Stimulating Cyber Security Information Diffusion.....	298
8.2.1	The benefits of information diffusion	298
8.2.2	Complementary roles of the triple helix.....	300
8.2.3	Recommendations	302
8.3.	The Law and Economics of Cyber Security.....	304

8.3.1	Connecting the two fields in this study	305
8.3.2	Barriers to building the bridge	306
8.3.3	Recommendations	309
8.4.	Closing Remarks	311
BIBLIOGRAPHY		315
	Bibliography	315
	Interviews	351
SUMMARY		357
SAMENVATTING		361
	EDLE PhD Portfolio.....	365
	Curriculum Vitae – Bernold Nieuwesteeg	367
	Personal Details.....	367
	Short bio.....	367
	Work experience	367
	Publications (selection).....	368
	Education.....	369
	Other professional activities	369

Biblioteka Główna
Akademii Sztuki Wojennej

26676/III (CB)



03-026676-000-0

The vast increase in digital insecurity - posed by ransomware, DDoS attacks and data breaches amongst others - requires an intelligent cyber security strategy. Government and industry can shape this strategy with legal instruments, such as regulations and contracts. However, very little is known regarding the social costs and benefits thereof. This is worrisome: cyber security expenditures will rise exponentially in the future as mankind becomes increasingly dependent on the digital world.

'The Law and Economics of Cyber Security' provides an in depth analysis into the root causes of this societal problem. The dissertation investigates novel legal instruments such as the possibility for insurance against cyber risks, the option to cover these risks by means of pooling and the EU data breach notification obligation in the GDPR. Furthermore, the study yields concrete policy recommendations for university, government and industry. In doing so, it combines fundamental analysis with concrete, actionable building blocks for an enhanced national cyber security strategy.

Bernold Nieuwesteeg is a Law and Economics researcher at Rotterdam Institute of Law and Economics (RILE), Erasmus University Rotterdam and has been a PhD researcher in the European Doctorate in Law and Economics (EDLE) Program. Bernold is partner at CrossOver, which offers cross company learning programs for mechanics, administrative personnel, social workers and trainees. He is a frequent contributor to the public policy debate in newspapers, conferences and public fora.

ISBN 978-90-8692-069-3



9 789086 920693 >

deLex 