THE IMPACT OF CYBERCRIME ON BELGIAN BUSINESSES
THE IMPACT OF CYBERCRIME ON BELGIAN BUSINESSES

Letizia Paoli
Jonas Visschers
Cedric Verstraete
Elke van Hellemont

intersentia
Cambridge – Antwerp – Portland

KU LEUVEN
CENTRE FOR IT & IP LAW
FOREWORD

This is the fourth book to be published in the series launched by the KU Leuven Centre for IT & IP Law (CiTiP) in 2018. The work collects the results of one of the work packages within the larger research project Belgian Cost of Cybercrime (BCC), funded by the BELSP0 – the Belgian Service Science Policy Office. BCC was a four-year interdisciplinary research project on the cost and impact of cybercrime in Belgium. The project started in December 2013 and ended in August 2018.

The project was set up on the basis of expertise gained by B-CCENTRE, which was the first main platform for collaboration and coordination with regard to cybercrime matters in Belgium. B-CCENTRE was initiated and coordinated by CiTiP’s predecessor ICRI and managed by Ann Mennens. It further comprised the collaboration of several academic research groups, industry players as well as public organisations (law enforcement, judges and policymakers).

The BCC project started from the assumption that, while information technology has been offering unprecedented opportunities to the Belgian society and economy, it also created new opportunities for, and vulnerabilities to, crime. Cybercrime can cause serious harm to individual and corporate internet users and compromise communication, e-commerce, financial and other services that rely on digital information and infrastructure. The BCC project aimed at systematically investigating and assessing the impact (i.e., costs or harms to material interests and non-material harms) of cybercrime on three levels: society, government and industry. Five teams of researchers at the KU Leuven and the University of Ghent have pooled their expertise in computer science (Distrinet and Cosic), criminology (LINC), communication sciences (MICT) and law (CiTiP), to jointly perform this research project under the coordination of the KU Leuven Centre for IT & IP Law (CiTiP).

The deliverables on the various work packages of the project are published on the website https://bcc-project.be/. The present book consists of an enhanced publication of the results of two survey waves amongst Belgium-based businesses carried out by researchers of the Leuven Institute of Criminology (LINC). We hope that it can provide useful information for policy makers and
industry players to make informed decisions and design strategies for enhanced protection against cyber threats.

Prof. dr. Marie-Christine JANSSENS
Head of Unit KU Leuven Centre for IT & IP law (GiTiP)

20 October 2018
ACKNOWLEDGEMENTS

Our study has been part of a broader multidisciplinary and multiannual research project aiming to assess the costs and harms generated by cybercrime to the Belgian society. This larger project has been funded by the BRAIN-be research program of the Belgian Science Policy Office (BELSPO) and has been coordinated by Prof. Marie-Christine Janssens of the KU Leuven Centre for IT and IP Law (CiTiP, previously known as KU Leuven Interdisciplinary Centre of Law and ICT (ICRI)). We warmly thank BELSPO for its generous funding and Prof. Janssens for her efficient and supportive coordination. We also thank the other project partners – and in particular Prof. Christophe Huygens and Vincent Rijmen from the Distirinet and COSIC Research Groups – for their useful inputs and feedback. We are also grateful to Edith Appelmans for the smooth administrative coordination of the project.

Furthermore, we owe much gratitude to the Federation of Enterprises in Belgium (FEB), and in particular Mr. Stefan Maes, as well as to the sector federations of Comeos and Febelfin for providing us with the necessary contact details of Belgian businesses. Last but not least, we thank the many business representatives who participated in the survey. Without these respondents openly sharing their cybercrime victimization experiences and the impact of such victimization on their businesses, this study would not have been possible.
CONTENTS

Foreword ............................................................. v
Acknowledgements .................................................. vii
List of Tables ......................................................... xi
List of Figures ......................................................... xiii
Introduction ........................................................ 1

Chapter 1.
Literature Review .................................................... 5
1.1. The definitions of cybercrime ................................. 5
1.2. Victimization, impact, costs and harms ...................... 8
  1.2.1. Victimization and its impact .............................. 8
  1.2.2. The costs of crime ........................................ 10
  1.2.3. The harms of crime ..................................... 12
1.3. The impact, costs and harms of cybercrime ................. 15
  1.3.1. A comparative overview ................................. 15
  1.3.2. Ponemon’s (2016) Cost of Cyber Crime Survey ....... 19
  1.3.3. PwC’s (2016) Global Economic Survey and Information
         Security Breaches Surveys (PwC UK, 2015; PwC Belgium,
         2017) .................................................................... 21
  1.3.4. Klahr et al. (2017)’s Cyber Security Breaches Survey .... 24
  1.3.5. Detica’s (2011) The Cost of Cybercrime ................. 26
  1.3.6. Anderson et al. (2013)’s Measuring the Cost of Cybercrime... 27

Chapter 2.
Conceptualization of the Key Concepts .......................... 31
2.1. Cybercrime ....................................................... 31
  2.1.1. Illegal access to IT systems ............................... 32
  2.1.2. Cyber espionage ............................................ 32
  2.1.3. Data/system interference .................................. 33
  2.1.4. Cyber extortion ............................................. 34
  2.1.5. Internet fraud .............................................. 35
2.2. The impact, harms and costs of cybercrime ................. 36
Chapter 3. 
Research Design ................................................. 39

3.1. Questionnaire ............................................. 39
3.2. Sampling procedures and final samples ................. 43
3.3. Scale construction ...................................... 46
3.4. Data analysis ............................................. 46

Chapter 4. 
The Results of the First Wave ............................... 49

4.1. Victimization in the past 12 months ....................... 49
4.2. Perceived risk of victimization in the subsequent 12 months .... 53
4.3. Costs (i.e., harms to material support) .................. 56
4.4. Harms to other interest dimensions ...................... 61
4.5. Expected harms of cybercrime .......................... 64
4.6. Preventive measures ...................................... 65

Chapter 5. 
The Results of the Second Wave ........................... 67

5.1. Victimization in the past 12 months ....................... 67
5.2. Perceived risk of victimization in the subsequent 12 months .... 70
5.3. Costs (i.e., harms to material support) .................. 73
5.4. Harms to other interest dimensions and comparison with harms 
to material support ........................................ 80
5.5. Expected harms of cybercrime .......................... 84
5.6. Preventive measures ...................................... 84

Chapter 6. 
Comparison of the Two Waves ............................... 93

Chapter 7. 
Conclusions, Research and Policy Implications .............. 103

7.1. Conceptualization and research design ................... 103
7.2. Key findings and discussion ............................. 105
7.3. Limitations .................................................. 108
7.4. Research and policy implications ......................... 111

References ......................................................... 121
Appendix ......................................................... 131
LIST OF TABLES

Table 1. Bearers and types of harms .................................................. 13
Table 2. Matrix for prioritizing harms, including scales of severity and incidence .................................................. 14
Table 3. Differences in victimization due to size and location (first wave) .................................................. 51
Table 4. Techniques used to commit cybercrime incidents (first wave) .................................................. 52
Table 5. Perceived victimization risk of cybercrime in next 12 months (first wave) .................................................. 53
Table 6. Differences in perceived victimization risk in the next 12 months due to business size, location and previous victimization (first wave) .................................................. 55
Table 7. Staff time invested in neutralizing the cyber incidents suffered (first wave) .................................................. 57
Table 8. Staff time invested in neutralizing the cyber incidents that was outsourced to external businesses or consultants (first wave) .................................................. 58
Table 9. Internal staff costs of the cyber incidents suffered (first wave) .................................................. 58
Table 10. Costs of hard- and software replacement for the cyber incidents suffered (first wave) .................................................. 59
Table 11. Value of other assets lost or damaged as a result of the cyber incidents suffered (first wave) .................................................. 60
Table 12. Fines and compensation payments as a result of the cyber incidents suffered (first wave) .................................................. 60
Table 13. Revenue lost as a result of the cyber incidents suffered (first wave) .................................................. 61
Table 14. Businesses’ assessments of the severity of the harms caused to other interest dimensions by the cyber incidents suffered (first wave) .................................................. 63
Table 15. Businesses’ assessments of the severity of the expected harms of cybercrime for their own sector (first wave) .................................................. 65
Table 16. Procedures to prevent cybercrime (first wave) .................................................. 66
Table 17. Differences in victimization due to size and location (second wave) .................................................. 69
Table 18. Techniques used to commit cybercrime incidents (second wave) .................................................. 69
Table 19. Perceived victimization risk of cybercrime in next 12 months (second wave) .................................................. 71
Table 20. Differences in perceived victimization risk in the next 12 months due to business size, location and previous victimization (second wave) .................................................. 72
Table 21. Parties responsible for the neutralization of cyber incidents suffered (second wave) ........................................... 74
Table 22. Internal staff costs of the cyber incidents suffered (second wave) . . . 75
Table 23. External staff costs of the cyber incidents suffered (second wave) . . 76
Table 24. Costs of hard- and software replacement for the cyber incidents suffered (second wave). ................................. 76
Table 25. Value of other assets lost or damaged as a result of the cyber incidents suffered (second wave). .......................... 77
Table 26. Fines and compensation payments as a result of the cyber incidents suffered (second wave). ............................... 78
Table 27. Revenue lost as a result of the cyber incidents suffered (second wave) .............................................................. 78
Table 28. Businesses’ assessment of the material harm caused by the cyber incidents suffered (second wave) ......................... 78
Table 29. Businesses’ assessments of the severity of the harms caused to all interest dimensions by the cyber incidents suffered (second wave) ............................................................... 79
Table 30. Businesses’ assessments of the severity of the expected harms of cybercrime for their own sector (second wave) ............... 82
Table 31. Frequency of procedures to prevent cybercrime (second wave) ..... 84
Table 32. Differences in victimization due to preventive measures (second wave) ........... ................................. 85
Table 33. Differences in small businesses’ victimization due to preventive measures (second wave) ........................................ 87
Table 34. Differences in medium and large businesses’ victimization due to preventive measures (second wave) ................. 88
Table 35. Perceived victimization risk of cybercrime in next 12 months in the two waves .......................................................... 90
Table 36. Costs resulting from the only/last cyber incidents suffered in the two waves ................................................................. 94
Table 37. Businesses’ assessments of the severity of the harms caused to other interest dimensions by the only/last cyber incidents suffered in the two waves ......................................................... 98
Table 38. Representation of significant changes in material and non-material harm assessments in the second wave vis-à-vis the first wave. ................................................................. 100
LIST OF FIGURES

Figure 1. The harm assessment process .................................................. 12
Figure 2. Incidence of cybercrime in the sample (first wave) ................. 50
Figure 3. Incidence of cybercrime in the sample (second wave) ........... 68
Figure 4. Incidence of cybercrime in the two waves ......................... 93