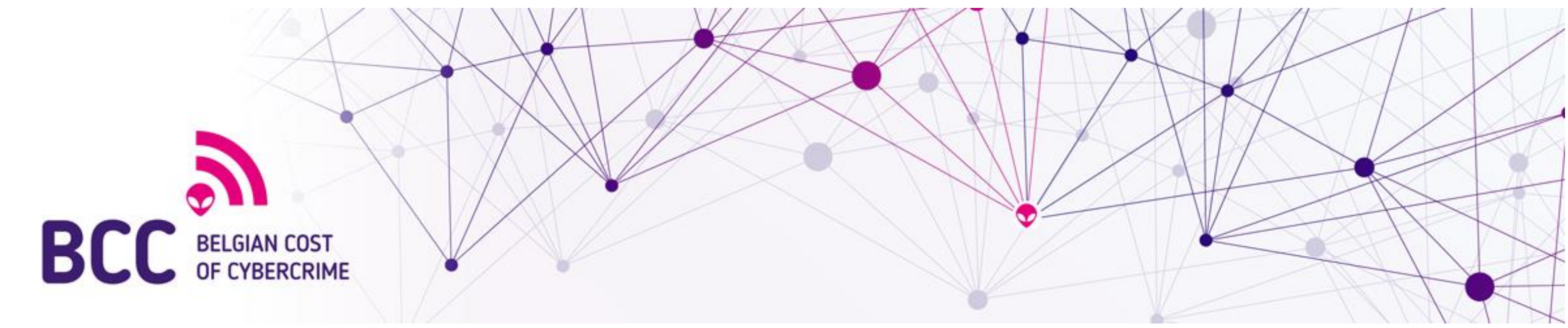

The Impact of Cybercrime on Belgian Businesses

KU LEUVEN
CENTRE FOR IT & IP LAW

belspo

LinC
LEUVEN INSTITUTE
OF CRIMINOLOGY

Preface

Information technology offers unprecedented benefits to the Belgian society and economy, but also creates new opportunities for, and vulnerabilities to, crime. As several dramatic cyberattacks on businesses and public bodies have recently shown (e.g., Granville, 2015, Goldman, 2017), cybercrime can cause serious harm to individual and corporate internet users, compromising their operational integrity, material interest, reputation and privacy. However, despite growing concerns, the costs and harms of cybercrime to individuals, businesses and government entities have - before the beginning of this project - not been systematically investigated in Belgium.

Thanks to funding from the BRAIN-be research program of the Belgian Science Policy Office (BELSPO), this project is intended to fills this gap. The KU Leuven Interdisciplinary Centre of Law and ICT (ICRI) (nowadays the KU Leuven Centre for IT and IP Law (CiTiP)), in collaboration with the KU Leuven Institute of Criminology (LINC), is the coordinator of the project. Other partners include, the UGent Research Group for Media & ICT (MICT), the KU Leuven iMinds-Distrinet Research Group (nowadays the KU Leuven imec-Distrinet Research Group), and the KU Leuven iMinds-COSIC Research Group (nowadays the KU Leuven imec-COSIC Research Group).

Specifically, the project aims to assess the costs and harms generated by cybercrime to the Belgian society, and to support the development of evidence-based and effective cybersecurity policies to help both, individual, and corporate internet users, better protect themselves.

The research project is divided into several work packages, which are coordinated by research departments of the KU Leuven, and Ghent University, under the guidance of the BELSPO follow-up committee. This report is the result of the fourth work package, which has been undertaken by CiTiP in cooperation with LINC. This work package intends to investigate and assess the victimization, cost and harms of cybercrime for the Belgian industry via a quantitative survey.

We thank BELSPO for funding the study and our partners within the BCC-project for their support. Furthermore, we are grateful to the Federation of Enterprises in Belgium (FEB), and in particular Mr. Stefan Maes, for providing us with the necessary contact details of over 8,000 Belgium-based (hereafter Belgian) businesses. Finally, 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 and would not have been possible.

Executive summary

This study is the first to systematically and empirically investigate cybercrime and the resulting costs and harms suffered by businesses located in Belgium (hereafter referred to as "Belgian businesses"; for initial attempts, see PwC Belgium, 2016 and 2017). It thus fills an important knowledge gap.

Unlike most other studies on the costs and impact of cybercrime, this study rests on a "technology-neutral" typology of cybercrime, i.e., a typology that is independent of the specific techniques used by cybercriminals. Our typology consists of five types of cybercrime that may potentially target businesses:

A. Unauthorized access to IT systems;

B. Corporate espionage;

C. Incidents causing an IT failure:

   1. IT failure due to data traffic (mostly caused by denial of service attacks)

   2. IT failure due to the manipulation of data and systems;

D. Cyber extortion; and

E. Internet fraud.

The first three types belong to the category of "computer-integrity crimes," that is, "new" crimes that can only be committed online. The latter two belong to the category of "computer-assisted crimes," which refers to "traditional" crimes that may be committed both offline and online. Our conceptualization of the three computer-integrity crimes is based upon the Council of Europe's 2001 Convention on Cybercrime, and the 2000 Belgian Criminal Act concerning cybercrime.[1] "Cyber extortion" has no direct counterpart in the Convention, rather, it is the cyber version of a standard offence in Belgian and other national criminal laws. The last type - "internet fraud" - comprises one of the two types of computer-related fraud defined by the Council of Europe's Convention—that is, fraud in online banking—but also includes two other more traditional types of fraud which frequently target businesses, namely, advance fee fraud and auction fraud.

Furthermore, we have conceptualized the impact of cybercrime in a novel and realistic way, drawing from Greenfield and Paoli's (2013) Harm Assessment Framework. This framework conceptualizes impact as the overall harm of cybercrime, that is, the "sum" of the harms to material support, or costs, and the harms to other interest dimensions.

As for the costs, we distinguish between personnel and other costs. For the personnel costs, we consider the man-hours spent to mitigate a cyber incident, the portion of them that has been outsourced, and the resulting costs. As for the other costs, we identify five categories: (1) hardware- and software replacement; (2) value of other lost or damaged assets (e.g., data files); (3) money paid to offenders[2]; (4) fines and compensation payments, and (5) revenues lost as a result of a cybercrime attack. Following Greenfield and Paoli (2013), we define "harms to other interest dimensions" as to harms to the

[1] Wet 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001.

[2] This category includes ransom, "protection money", and "hush money", the latter consisting of a sum paid to buy the "silence" of cybercriminals after the theft of confidential data of a business). It is only applicable to cyber extortion.

business's functional integrity—which we split into internal operational activities and services to customers—reputation and "privacy. Harms to privacy might be caused b, unauthorized access and misappropriation of a business's sensitive or proprietary information, which might reduce its ability to pursue its institutional interests. Driven by the realization that these harms cannot be monetized, we have asked the respondents to assess their severity on the basis of a six-point scale including the categories of *no harm, marginal, moderate, serious, grave,* and *catastrophic.*

Using the above framework and concepts, we subsequently developed a survey questionnaire to investigate the following five key topics:

(1) the prevalence of businesses' victimization and the incidence of the five types of cybercrime, in the past 12 months;

(2) the businesses' perceived risk of cybercrime victimization in the next 12 months;

(3) the costs (that is, the harms to material support) generated by the five types of cybercrime;

(4) the non-material harm of the same cybercrime types;

(5) the expected impact of cybercrime on the sector related to each business.

This study also considers the extent to which the incidence of cyber incidents, and the severity of the resulting material and non-material harms, as well as the perceived victimization risk depend on the businesses' size, location, and/or previous victimization experiences.

In the spring and summer of 2016, we sent automatically generated emails, with codes to access and resume the survey, to 8.051 members of the Federation of Enterprises in Belgium (FEB) - the largest employers organization in Belgium. In total, 453 company representatives completed the survey, resulting in a sample of 310 respondents, after the removal of incomplete or unusable questionnaires.

Victimization and incidence: The survey results indicate that a large number of businesses are victims of cybercrime. In total, two thirds (67%) of the businesses report that they were a victim of at least one of the five types of cybercrime during the last 12 months. Almost half of the businesses have experienced unauthorized access to IT systems (50%), and incidents resulting in IT failure (46%). Less than a quarter report experience with the other three types of cybercrime: cyber extortion (24%), internet fraud (13%) and corporate espionage (4%). A majority of the businesses reporting victimization indicate that they have been attacked more than once. For example, 41.6% of the respondents reported multiple incidents of unauthorized access to IT systems, 32% multiple incidents resulting in IT failure and 13.8% multiple incidents of cyber extortion. With regards to unauthorized access to IT systems, incidents resulting in IT failure, and cyber extortion, our findings suggest that smaller businesses (i.e., businesses with less than 50 staff) are victimized less often than larger ones.

Perceived risk of victimization: The businesses generally assess their risk of victimization in the 12 months following the date of their response, as "very unlikely" or "unlikely." Only unauthorized access to IT systems through "hacker"-tools and -techniques is perceived as considerably more likely to happen in the next 12 months. For this subtype of cybercrime, approximately 60% of the respondents assess the risk of victimization of their business's in the next 12 months as "likely" or "very likely." With reference to unauthorized access to IT systems, incidents resulting in IT failure, and cyber extortion, the businesses that have already been victimized predict a higher risk of cyberattacks in the following 12 months, compared to the non-victimized businesses.

Costs:[3] The large majority of the incidents are solved in less than one day (unauthorized access to IT systems: 82%; incidents resulting in IT failure: 80%; cyber extortion: 68%). However, between 20% and 30% of the incidents require more than one day to be neutralized. Most of the reported incidents are addressed by the internal staff. Outsourcing occurs in less than half of all incidents, but the neutralization of IT failure incidents is outsourced more frequently than that of other types of cybercrime. The internal staff costs for neutralizing cybercrime incidents tend to be rather low, particularly in the case of unauthorized access: for the three crime types, at least 70% of the victimized businesses report cost not higher than €229. However, considerable minorities (that is, 10% of the businesses victim of unauthorized access, 16% of those victim and incidents resulting in IT failure and 23% of those victim of cyber extortion) report costs higher than €458 for the neutralization of the last or most serious incident.

The other non-personnel costs are also usually low. For example, more than half of the businesses bear no costs for replacing hardware and software, after suffering unauthorized access to their IT system (56%), incidents resulting in IT failure (58%), or cyber extortion (67%). However, between 2% and 4% of the businesses report replacement costs of €10,000 or more due to unauthorized access to their IT system (4.0%), incidents resulting in IT failure (3%), or cyber extortion (1.5%).

Over 70% of the businesses that are victims of cyber extortion, report no other lost or damaged assets, whereas the percentage decreases to 50%, in the case of incidents resulting in IT failure.[4] Only 1.6% and 9% of the businesses suffering cyber extortion and incidents resulting in IT failure, report that the value of the stolen or damaged assets was €10,000 or more. However, about half of the 9% of businesses reporting such costs for cyber extortion respectively, indicate that the assets lost or damaged are worth more than €100,000.

Among the victims of cyber extortion, 94% indicate that they have paid no money to offenders.

Likewise, more than 90% of the businesses suffering unauthorized access to their IT system, incidents resulting in IT failure, or cyber extortion, indicate that they have not paid any fines or compensation to injured parties (91%, 93% and 91%, respectively).

A majority of the victimized businesses also indicate that they have not lost any revenue because of a cyber incident, but there are considerable differences between one type of cybercrime and another. The percentage of businesses experiencing no loss is highest in the case of unauthorized access (77%), followed by cyber extortion (73%), and incidents resulting in IT failure (62%). However, between 11% and 24% of the businesses estimate losing between €1 and €9,999 because of one of these cyber incidents. Fewer businesses admit to having suffered bigger losses: 3% report revenue losses between

[3] Whereas in the report we also discuss the absolute figures for corporate espionage and fraud, here we focus on the data concerning: the costs and harms of unauthorized access to IT systems, incidents resulting in IT failure, and cyber extortion, for which we have more reliable data.

[4] We have investigated this cost only for these two cybercrime types and corporate espionage.

€10,000 and €49,000; between 1% and 3% report losses of €50,000, or more, for unauthorized access, and incidents resulting in IT failure, respectively.

Non-material harm: For the three cybercrime types for which we have substantial data (i.e., unauthorized access to IT systems, incidents resulting in the failure of IT systems and cyber extortion), the victimized businesses consistently report that internal operational activities are more seriously affected than the other three dimensions namely, services to customers, reputation and privacy. In fact, about half of the businesses victimized, report no harm to these last three dimensions as a consequence of unauthorized access to IT systems (service to customers: 52%; reputation: 49%; privacy: 49%), incidents resulting in IT failure (service to customers: 45%; reputation: 45%; privacy: 58%) or cyber extortion (service to customers: 46%; reputation: 58%; privacy: 56%). Instead, at most a third of the businesses victimized report no harm to their internal operational activities as a consequence of the same crimes (unauthorized access to IT systems: 33%; incidents resulting in IT failure: 18%; and cyber extortion: 20%). Even for the services to customers, reputation and privacy, between 35% and 45% of the victimized businesses report marginal or moderate harm to these three interest dimensions, and 5-10% of them report having experienced serious or grave harm to them. Moreover, in the case of cyber extortion, 3%, 2% and 3% of the businesses victimized report catastrophic harms to the services to customers, reputation and privacy.

Between 50% and 65% of the business victims of unauthorized access to their IT system, incidents resulting in IT failure or cyber extortion report marginal or moderate harm to their internal operational activities. Furthermore, between 14% and 20% of them report serious or more harm to their internal operational activities. In the case of unauthorized access to IT systems 14% of the businesses report serious or grave harm and 1% catastrophic harm. For incidents resulting in IT failure, 18% of the businesses report serious or grave harm and 1% catastrophic harm. In the case of cyber extortion, 17% of the businesses describe the harm suffered as serious or grave, while 5% admit to have suffered catastrophic harm.

In a nutshell, cybercrime occurs frequently but as of summer 2016, it did not generate serious costs and harm for most businesses. However, a minority of the businesses victimized did suffer serious, grave or even catastrophic harm, particularly to their internal operational activities, as a result of cyber extortion.

While, at first these results appear “lower” than those reported by private security and consultancy companies, they are consistent with the studies conducted by academics on behalf of government agencies (e.g., Anderson et al., 2013; Klahr et al., 2016)

Expected impact: The businesses participating in the survey are well aware of the potential impact on cybercrime on their sector—and in light of the earlier findings might even overestimate the threat represented by cybercrime. For all dimensions of interest, except material support and finances, about 50% of the businesses expect harm to their internal operational activities, reputation, and privacy of other businesses in their sector, to be at least serious.

Limitations of the study: This is the first academic study in Belgium that has been conducted on this topic. It is, therefore, not possible to compare the results with those of previous studies and further research is necessary to understand how businesses protect themselves from a phenomenon – cybercrime – that rapidly evolves and seems to become more threatening. In addition, it is important to keep in mind that the respondents are not representative of all Belgian businesses. At least for certain types of cybercrime, businesses might also not be aware of cyberincidents and/or the resulting harms and costs or might not be willing to admit them in a survey.