BCC BELGIAN COST OF CYBERCRIME

The Impact of Cybercrime on Belgian Businesses

Letizia Paoli, Jonas Visschers,
Cedric Verstraete en Elke van Hellemont

September 2017

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 fill 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, as well as to the sector federations of Comeos and Febelfin for providing us with the necessary contact details of 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. Illegal access to IT systems;

B. Corporate espionage;

C. Data and system interference;

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 business's functional integrity—which we split into internal operational activities and services to customers—reputation and "privacy." Harms to privacy might be caused, for example, by illegal 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

[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.

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 perceived victimization risk depend on the businesses' size, location, and/or previous victimization experiences (in the latter case).

In the spring and summer of 2016, we sent automatically generated emails, with codes to access and resume the survey, to 9,249 representatives of Belgian businesses. In total, 453 business representatives completed the survey. The questionnaires of 310 of them could be retained for statistical analyses. Albeit low, our response rate is in line with those of the few studies that have made their response rate public (e.g., CSI, 2011). Our sample is bigger than those of two earlier studies that provided preliminary data on the impact of cybercrime on Belgian businesses (e.g., PwC-Belgium, 2016).

Our results can be summarized as follows:

Victimization and incidence: The survey results indicate that a large number of businesses are victims of cybercrime. In total, two thirds (66.5%) 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 illegal access to IT systems (50%), and data/system interference (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. With regards to illegal access to IT systems 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 illegal access to IT systems through hackertools 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 illegal access to IT systems, data/system interference, 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 last or only incidents are resolved in less than one day (illegal access to IT systems: 82%; data/system interference: 80%; cyber extortion: 68%). However, between 20% and 30% of the incidents require more than one day to be neutralized - a percentage that grows up to more than 49% for all incidents of illegal access recorded in the last 12 months. Most of the reported incidents are addressed by the internal staff. Outsourcing occurs in less than half of all incidents, but the neutralization of incidents of data/system interference is outsourced more frequently than that of other types of cybercrime; there are no substantial differences between the only or last and the most serious incidents.

The internal staff costs for neutralizing cybercrime incidents tend to be rather low: for the three crime types for which we have better data (i.e., illegal access to IT systems, data/system interference, and cyber extortion), more than half of the victimized businesses report costs not higher than €229 due to the only or last incident. In the case of illegal access to IT systems this percentage goes up to more than 70%.

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 illegal access to their IT system, data/system interference, or cyber extortion. However, between 1.5% and 4% of the businesses report replacement costs of €10,000 or more due to the only or last incident of illegal access to their IT system, data/system interference, or cyber extortion.

Half of the businesses that are victims of cyber extortion report no lost or damaged assets. For data/system interference, this percentage goes up to 60% for the most serious incident, and 70% for last or only incident.[4] Only 9% of the businesses suffering cyber extortion report costs of €10,000 or more; for data/system interference, the percentage is in all cases lower than 3%.

Among the victims of cyber extortion, 94% indicates that they have paid no money to offenders. For the latter crime as well as for illegal access (only/last and all), and the only/last incidents of data/system interference, more than 90% of the businesses report paying no fines or compensation to injured parties. Only for the most serious incidents of data/system interference, the percentage slightly decreases to 86%.

Finally, a large majority of the businesses also indicate that they have not lost any revenue because of cyber incidents, even if there are considerable differences from one cybercrime type to the other. The percentage experiencing no loss is the highest for illegal access to IT systems (only/last: 77%; all: 72%), followed by cyber extortion (only/last: 73%), and data/system interference (only/last: 62% and most serious: 60%). However, between 11% and 24% of the businesses estimate losing between €1 and €9,999 because of one of these three cybercrime types. Much smaller percentages of businesses confronted with illegal access to IT systems and data/system interference admit suffering losses of €10,000 or more.

Non-material harm: The businesses suffering illegal access to their IT system, data/system interference and cyber extortion consistently report that internal operational activities are more seriously affected

[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 illegal access to IT systems, data/system interference, and cyber extortion, for which we have more reliable data.

[4] We have investigated this cost only for data/system interference, cyber extortion and corporate espionage.

than the other three dimensions namely, services to customers, reputation and privacy. Between 41% and 66% of the businesses victimized, for example, report no harm to these last three dimensions. Instead, the percent of no harm decreases to about 20% in the case of internal operational activities.

Even for the services to customers, reputation, and privacy, between 35% and 50% of the victimized businesses report marginal or moderate harm to these three interest dimensions, with slightly higher percentages for all the incidents of illegal access and the most serious cases of data/system interference. Five to ten percent of victimized businesses have experienced serious or grave harm to one or more of these three interest dimensions, a percentage that goes up to 13.4% for service to customers after the most serious incident of data/system interference. Moreover, in the case of cyber extortion, small percentages of the businesses victimized (< 5%) suffer catastrophic harms to the services to customers, reputation, and privacy.

Respondents consistently rank the harms to internal operational activities higher. With the exception of the only or last case of illegal access to IT systems (around 33%), the percent of businesses suffering no harm to internal operational activities is only 20%. Between 50% and 63% of the victimized businesses have experienced marginal or moderate harm to their internal operational activities, and between 14% and 20% report serious or grave harm. About 1% of the victimized business even admit catastrophic harm to their internal operational activities because of illegal access or data/system interference.[5] For cyber extortion, the percentages are higher. For the last/only incident of this cybercrime type, 17% of the businesses describe the harm suffered as serious or grave, and 5% admit having suffered catastrophic harm.

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.

In a nutshell, business-related cybercrime occurs frequently but as of summer 2016, it did not generate serious costs or harm for the majority of businesses based in Belgium. However, a minority of the victimized businesses assess the harms to one or more interest dimensions as serious or more. Less than 10% of victimized business report such harm for the interest dimensions of services to customers, reputation, and privacy; only for the most serious incidents of data/system interference, such percentage goes up to 14% with reference to services to customers. Businesses generally rank the harms to their internal operational activities higher: 15% to 22% of them rate the harms to their internal operational activities as serious or more. In the case of cyber extortion, a few of the victimized businesses even report catastrophic harm, with the highest percentage being recorded for internal operational activities (4.5%). Cyber extortion thus appears to be the most harmful of the cybercrime types considered.

Our findings are more conservative than those reported by private security and consultancy companies, but appear to be higher than those reported by other academic studies, even if they are not directly comparable (e.g., Anderson et al., 2013; Klahr et al., 2017). We can only speculate about the source of

[5] In all these cases, there are no major differences between last/only and all/most serious incidents.

the differences, given the different period and national context of the studies and the different methodologies adopted. The difference, in particular, might be due to the clear distinction between costs and harms in our typology; this might have encouraged businesses to report harms that previously remained hidden, because the businesses were forced to provide a monetary estimation of such harm.

Despite the methodological limitations of survey research, the use of a convenience sample and the low response rate, the study constitutes —thanks to its innovative conceptualization and operationalization of cybercrime, impact, cost and harm--the first, independent, rigorous assessment of the costs and harms suffered by Belgium-based businesses because of cybercrime.

List of Tables

List of Figures

Contents

Introduction

Nowadays, governments and businesses all over the world consider cybersecurity a top priority and are spending billions of dollars and euros to protect themselves and the public from cybercrime (e.g., Volz, & Hosenball, 2016). Since the 2007 cyberattacks against Estonia, news of other devastating cybercrimes have been published at an ever increasing pace, alerting even the average media consumer that cybercrime can cause serious harm (e.g., Granville, 2015). In particular, the attacks on the Japanese conglomerate Sony in 2012, the German Parliament in 2015 (e.g., Boie, 2015), Bangladesh National Bank (Corkery, 2016, April 30) and the US Democratic National Committee in 2016 (Lipton, Sanger & Shane, 2016, December 13) as well as the repeated attacks on Ukraine's infrastructures and ministries (Zinets, 2017, February 15) have vividly demonstrated that cybercriminals can gravely compromise the communication, reputation, activities, and even the sheer functional integrity, of virtually all businesses, NGOs, and public sector entities, in both the developed and developing world. In May 2017, an audacious cyberattack crippled more than 200,000 computers in more than 150 countries, using a new strain of ransomware, known as WannaCry. Among the companies and government agencies affected were FedEx, Britain's National Health Service and the Russian Interior Ministry (e.g., Goldman, 2017, May 12).

Over the past few years, in Belgium too, the phenomenon of cybercrime has received growing media attention and provoked concern (e.g., Wauters, 23.08.2017, p. 3). To allay these fears and protect its citizens, businesses, and other entities, in 2014 the Belgian government set up the Centre for Cybersecurity Belgium (http://www.ccb.belgium.be/en), which became operational in 2015, and has classified cybercrime as a top priority in its long-term security plan - the Kadernota Integrale Veiligheid 2016-2019 (Federale Regering, 2016).

Despite these steps, little empirical data is available to investigate the experiences of Belgium-based (hereafter Belgian) businesses with cybercrime, or the impact cybercrime has had on these businesses (e.g., PwC Belgium, 2016 and 2017). The present study aims to fill this gap.[6] In particular, it intends to achieve two aims:

- First, to assess the prevalence of cybercrime victimization and the incidence of cybercrime incidents among Belgian businesses in the past 12 months as well as the businesses' perceived risk of victimization in the upcoming 12 months.
- Second, to determine the impact, and expected impact, of these cybercrime types on Belgium businesses.

Our study captures five types of cybercrime: (1) illegal access to IT systems; (2) corporate espionage; (3) data/system interference; (4) cyber extortion, and (5) internet fraud. Unlike many others (e.g., CSI, 2015; Ponemon, 2015; HP, 2016), our typology is technology-neutral, i.e., it is independent of the specific techniques used by cybercriminals; it also largely draws, and is therefore compatible with, the juridical definitions of cybercrime.

For the impact assessment, we have relied on Greenfield and Paoli's (2013) harm assessment framework to conceptualize impact in a novel way: we let the survey respondents assess the severity of the impact of the different types of cybercrime they experienced. In line with Greenfield and Paoli's

[6] The problem is not only limited to Belgium. In an authoritative study on the impact of cybercrime in the UK, Anderson et al. (2013, p. 267) also noted that reliable cybercrime data – if available – is "still insufficient and fragmented." This assessment is repeated by others (see for example Diamond & Bachmann, 2015, p. 27).

(2013) framework, we understand the impact of cybercrime as the overall harm of cybercrime, that is, the "sum" of the harms to material support, or costs, and the harms to other interests generated by cybercrime. Whereas the harms to material support can be monetized and therefore are cost, the harms to other interest dimensions cannot be monetized. Rather than relying on arbitrary assumptions to provide a monetary estimate of all harms, we have asked our respondents to rate non-material harms on the basis of a six-point scale, ranging from *none* to *catastrophic*. This study also considers the extent to which the incidence of cyber incidents, and the perceived victimization risk depend on the businesses' size, location, and/or previous victimization experiences (in the latter case).

This report is structured as follows. In the first chapter, we begin with a literature review that discusses three issues: previous definitions of cybercrime; the different literatures on cost; impact and harms of crime, and the related methods of measurement and assessment, and finally, previous studies attempting to estimate the cost, impact and harms of cybercrime. In the second chapter, we present our conceptualization of cybercrime and its impact. In the third, we describe the project research design, including the survey with which we have operationalized the key concepts; our sample; the scale construction; and data-analysis. In the fourth chapter, we discuss the main findings in the following order: (1) prevalence of cybercrime victimization and the incidence of cybercrime in the past 12 months, (2) perceived risk of victimization by cybercrime in the upcoming 12 months, (3) material harms (i.e., monetary costs) of cybercrime, (4) non-material harm of cybercrime and (5) expected impact. In the conclusion, we summarize the main findings and formulate policy recommendations.

1. Literature Review

Our literature review consists of three parts. First, we consider the main juridical and academic definitions of cybercrime. Second, we briefly discuss the different bodies of literature on the cost, impact and harms of crime, as well as the related methods of measuring and assessing them. Third, we critically review the previous studies attempting to estimate the cost, impact and harms of cybercrime.

1.1. The Definitions of Cybercrime

As many other broad categories of crime[7], cybercrime too, is a contested concept. There is no consensus regarding the definition of cybercrime, either in the academic literature (e.g., Clough, 2015; Wall, 2007), or in legal and policy documents. As noted in a 2013 review of the UN Office on Drugs and Crime (UNODC, 2013), many of these documents do not even define cybercrime per se, but identify specific acts that constitute cybercrime. To confuse matters further, the terms "computer," "e-," "internet," "digital" and "information crime," are often used substitutes for cybercrime. Hence, for example, Clough (2015, p. 9) states that "there are almost as many terms to describe cybercrime as there are cybercrimes." Along similar lines, Van der Hulst & Neve (2008, in Leukfeldt et al., 2013, p. 2) conclude:

> A common definition and conceptual framework is lacking for this field of crime. A veritable arsenal of terminology is used, sometimes in combination with the prefixes cyber, computer, e-, internet, digital or information. Terms are bandied around, applied randomly, reflect overlap in content or reflect important gaps.

For researchers, the lack of a clear definition is problematic. A shared definition would not only help delineate the scope of the problem under investigation, but also facilitate discussions among scholars and provide a basis for comparing their research findings (ENISA, 2016a, p. 82; Gordon & Ford, 2006, p. 13). This definitional cacophony at least partially reflects the fact that cybercrime is studied from a wide variety of disciplines, ranging from social sciences to computer sciences (Jaishankar, 2010). Computer scientists and security companies, for example, tend to use a rather technical lexicon unfamiliar to many conventional social scientists. In addition, these "technological" studies often emphasize specific techniques (e.g., malware or phishing) that can be deployed in order to commit several offences labelled as cybercrime in criminal law. Certain types of malware, for example, can be used for system interference, but also to gain illegal access to an IT system, or to log keystrokes of unsuspecting users (Van der Hulst & Neve, 2008; VU Amsterdam & PwC, 2014). Furthermore, offenders in cyberspace often combine different techniques to achieve their ultimate purpose, e.g., inducing an IT failure (Wall, 2007).

Despite this cacophony, many policymakers and researchers agree about the distinction between "computer-assisted" and "computer integrity" crimes (e.g., Wall, 2007, pp. 49-50, European Commission, 2013, p. 3), even if they may use slightly different terms for indicating these two categories. The first category consists of crimes whereby information technology mainly functions as a tool to commit already existing crimes such as fraud or extortion. In contrast, the second category consists of new crimes directly targeting the integrity of information technology that came into existence with the rise of computers and the internet. Data or system interferences are examples of this second category (Clough, 2015; De Cuyper & Weijters, 2016; Kerkhofs & Van Linthout, 2013; Leukfeldt, de Pauw, Domenie & Stol, 2011; Van der Hulst & Neve, 2008).

[7] For examples of organized and white-collar crime, see Paoli & Vander Beken (2014) and Van Erp, Huisman & Vande Walle (2015).

Crimes belonging to the first category - "computer-assisted" crimes - are generally covered by the traditional criminal legislation (e.g., Kerkhofs & Van Linthout, 2013). The second category of computer-integrity crimes began to be legally defined in the Council of Europe's 2001 Convention on Cybercrime[8].

This Convention identifies five "offences against the confidentiality, integrity and availability of computer data and systems:" "illegal access" (art. 2),[9] "illegal interception" (art. 3),[10] "data interference" (art. 4),[11] "system interference" (art. 5)[12] and "misuse of device" (art. 6).[13] It further defines two so-called "computer-related offences," including, "computer-related forgery" (art. 7)[14] and "computer-related fraud" (art. 8).[15] Further, the convention identifies two additional categories, namely, "content-related offences", i.e. child pornography (art. 9), and "offences related to infringements of copyright and related rights" (art. 10). It must be noted, though, that the Convention's definitions of computer-related forgery and fraud do not refer to the traditional offence of forgery and fraud in national criminal law. Especially in the case of fraud, it is clear that the definition of computer-related fraud given by the Convention is only a very small sub-set of the multiple variants of frauds that are committed "offline" (Levi, 2013), and does not even cover the many types of computer-assisted, or computer-related frauds, discussed in the literature and other policy-documents (e.g., Anderson et al. 2013). The two types of fraud defined by the Convention, moreover, straddle the distinction between "computer-related" and "computer-integrity" crimes, as they are defined as "computer-related" but involve either "input, alteration, deletion or suppression of computer data" or "interference with the functioning of a computer system" (art. 8).

Whereas the Council of Europe does not define cybercrime per se, the European Commission has at least vaguely defined cybercrime in a footnote of the 2013 Cybersecurity Strategy of the European Union, as "a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (European Commission, 2013, p. 3). This definition, as well as the whole strategy are however non-binding for the Member States. In the strategy as well as in a 2007 Communication towards a general policy on the fight against cybercrime (European Commission, 2007), the Commission advances a tripartite classification of cybercrime. Accordingly, "cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related

[8] Convention on Cybercrime, Council of Europe, Budapest, November 23th 2001, *E.T.S.*, nr. 185.

[9] Illegal access is defined as "the access to the whole or any part of a computer system without right" (Convention on Cybercrime, 2001, art. 2).

[10] Illegal interception is defined as "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data" (Convention on Cybercrime, 2001, art. 3).

[11] Data interference is defined as "the damaging, deletion, deterioration, alteration or suppression of computer data without right" (Convention on Cybercrime, 2001, art. 4).

[12] System interference is defined as "the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data" (Convention on Cybercrime, 2001, art. 5).

[13] Misuse of device is defined as "the production, sale, procurement for use, import, distribution or otherwise making available of: a) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; b) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5" (Convention on Cybercrime, 2001, art. 6).

[14] Computer-related forgery is defined as "input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible" (Convention on Cybercrime, 2001, art. 7).

[15] Computer-related fraud is defined as "the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; or b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person" (Convention on Cybercrime, 2001, art. 8).

offences (e.g. online distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)" (European Commission, 2013, p. 3). As the Council of Europe's Convention, the European Commission's classification also includes content-related offences. However, it extends this category, as it mentions incitement to racial hatred, in addition to child pornography.

Since the turn of the twenty first century, computer-integrity crimes have been introduced in the penal codes of most countries (see UNODC, 2013 for a review). Well aware of what would be included in the Council of Europe's Convention, in 2000 Belgian legislators adopted an act on cybercrime[16] that (among other things) created four specific cyber offences. The first two new offences of hacking[17], and IT sabotage[18], correspond to the offences of illegal access and data as well as system interference, defined by the Council of Europe's 2001 Convention under the title of computer-integrity crimes (Kerkhofs & Van Linthout, 2013). The offences of IT forgery[19] and IT fraud[20] belong to the second category of "computer-related offences" in the Council of Europe's 2001 Convention.

1.2. Victimization, Impact, Costs and Harms

The concepts of impact, cost and harm of crime are also not well defined and are often used interchangeably in both the academic and policy discussions. A brief comparison of the two Serious and Organized Crime Threat Assessments published so far by Europol (2013 and 2017), gives a good illustration of this conceptual confusion and interchangeability. The 2013 SOCTA (Europol, 2013) used "harm" as its pivotal concept, discussing the harms of each of the selected criminal activities in separate subsections. Despite no intervening changes in EU law or policy documents, the 2017 SOCTA mentions the term "harm" only twice, and uses "threat" and "impact" as its key concepts.

In the following subsections, we first discuss the different bodies of literature concerning impact, cost, and harm of crime along with methods for their measurement and assessment. In our discussion of impact, we also include the concept of victimization, which is related to, and logically precedes, the three other concepts, and is mostly closely linked with impact.

1.2.1. Victimization and its impact

The concept of victimization is the most straightforward of the four selected terms: it refers to the process and experience of being victim of a crime. Impact is the most generic of the four and is mostly not (carefully) defined.

Driven by the growing societal concern for victims and their growing media visibility and policy relevance, research on crime victimization, and its impact, has expanded dramatically since the 1970s, leading to the creation of a separate discipline, victimology (e.g. Walklate, 2007). Since the 1960s, victimization surveys have become the main instrument to estimate the incidence of victimization of ordinary crimes, that is, the extent to which the general public has been victim of certain crimes over a period of time (e.g., ICVS; Mayhew & Van Dijk, 2014). The data produced by victimization surveys have since the 1980s been recognized as an alternative measure of crime that is a useful supplement to police and official statistics. Addressing a sample of the general population, victimization surveys mostly focus

[16] Wet 28 november 2000 inzake informaticacriminaliteit, *BS* 3 februari 2001.
[17] Art. 550*bis* Sw.
[18] Art. 550*ter* Sw.
[19] Art. 210*bis* Sw.
[20] Art. 504*quater* Sw.

on ordinary crimes where the victims are individuals or households. Information on consensual or "victimless" crime (i.e., drug use, prostitution, gambling), and corporate - white-collar crime, is typically not collected through victimization surveys, such as the National Crime and Victimization Survey[21], or the Belgian Veiligheidsmonitor (Safety Monitor)[22].

Since the 1990s, surveys have also been conducted to assess the victimization experienced by businesses, becoming a powerful tool for assessing their experiences with crime and safety as well as their perceptions and attitudes (e.g., PwC, 2016b, Williams, 2016). These surveys indicated that businesses are exposed to crime more than individuals and households, especially with regards to the risk of being victimized by organized crime, bribery/corruption, fraud, counterfeiting, requests for protection money, intimidation, and extortion. According to a UN Manual (United Nations Office on Drugs and Crime and United Nations Economic Commission For Europe, 2010, p. 198) on the topic, business victimization surveys may have the following objectives:

- to assess the type and extent of crimes committed against businesses;
- to assess the impact of crime and corruption on businesses and relevant costs;
- to assess the preventive measures taken by businesses as well as their willingness to engage in crime prevention initiatives with the local community;
- to assess the perceptions and attitudes of the private sector on a wide range of crime and corruption related issues.

In addition to victimization surveys, numerous studies have— mostly in a qualitative way—explored the impact of a broad range of individual victimizations. In reviewing these studies, Spalek (2006, pp. 68-79) distinguishes the psychological, emotional, behavioral, financial, and physical impact of different types of crime on the victim, but this body of research has been largely descriptive, with most studies focusing on a specific experience of victimization (e.g., Resick, 1990; Stanko & Hobdell, 1993) or specific impacts (e.g., the household's moving decision in Dugan, 1999). This literature has been criticized for focusing almost exclusively on traditional crimes and its individual victims (e.g., Fattah, 2010, pp. 54-57). Correspondingly, most studies on victimization have given little attention to corporate crimes and other offences lacking immediate individual victims, and neglected non-individual bearers of harm (Fattah, 2010, pp. 54-57; Whyte, 2007).

The term "impact" is also used in several studies, considering the effect of criminal victimization on businesses and other entities. Kopp and Besson, (2009), Levi and Burrows (2008) and Levi, Innes, Reuter and Gundu (2013), for example, have considered the impact of organized crime activities. In these studies, and others specifically focused on cybercrime (see infra), impact is de facto operationalized largely or exclusively in terms of social cost. In line with the cost-of-crime literature, several studies (e.g., Kopp & Besson, 2009) also include the costs of societal reactions.

1.2.2. The Costs of Crime

Since the 1970s, a relatively large body of economic literature has grown about the costs of crime. This literature equates the costs, with the harms of crime. Following Cohen (2005, pp. 9-11), such literature has traditionally distinguished three categories: the costs caused by criminal behavior; those incurred by society in response to crime either to deter or prevent future incidents or to exact retribution; and

[21] https://www.bjs.gov/index.cfm?ty=dcdetail&iid=245.
[22] http://www.moniteurdesecurite.policefederale.be/veiligheidsmonitor/

those incurred by the offender. More recently, Wickramasekera et al. (2015) offer a slightly different categorization and posit that costs can be calculated according to victim's perspective, government perspective and societal perspective. Victims' perspective consists of costs incurred by the victims; the government perspective accounts for the costs incurred by the criminal justice system, whereas the societal perspective is comprised of both earlier categories and also includes costs to taxpayers and offenders.[23]

In both classifications, the first category of costs—that is, the costs directly caused by criminal behavior—is further split by economists into three subcategories: direct, indirect, and intangible costs. Direct costs can be distinguished from indirect and intangible costs, because they involve a monetary exchange, for example, the cost of repairing a car damaged by a crime. Indirect costs refer to the economic value of consequences of crime that do not involve a direct monetary exchange, such as loss in productivity. Fear, pain, suffering, and lost quality of life are the most important intangible costs for individual victims. For businesses, and other entities intangible costs involve loss in customer goodwill or drops in employee morale. Intangible costs are the most difficult to quantify (Wickramasekera et al., 2015) and for some scholars (e.g., Caulkins, Reuter and Coulson, 2011; Paoli & Greenfield, 2013), it is also inherently impossible to do so.[24]

For the most part, the earliest studies on cost of crime did not go beyond the out-of-pocket direct and indirect costs of victimization. Thaler (1978) was the first to attempt to account for "intangible" costs. Whereas Thaler (1978) used a method known as "hedonic valuation" to focus on differences in property values in high-crime and low-crime areas, several other methods have been proposed since then. These include value-of-life estimates (Phillips & Votey, 1981), jury award data to develop monetary estimates of pain, suffering, and lost quality of life (Cohen, 1988), "contingent valuation"—that is, asking potential victims how much they would pay to avoid certain crimes (e.g., Cohen, Rust, Stehen & Tidd, 2004)—and "value of statistical life," which provides a means to identify society's willingness-to-pay for a small reduction in the risk of death (e.g., Viscusi, 2008; Viscusi & Aldy, 2003).[25] As Paoli and Greenfield (2013) argue, "each of these methods, although capable of shedding light on one or more dimensions of harm, has its drawbacks in contributing to a complete measure" (see also Heaton, 2010 for a critical discussion). According to some authors, it is inherently impossible to express in monetary terms harms to dignity, privacy and autonomy, for either individuals or corporate entities. Therefore, it is impossible to express all harms of crime by reducing them to single, monetary, or other measure (e.g., Zimring & Hawkins, 1995; Caulkins et al., 2011; Paoli & Greenfield, 2013). Others are also opposed to the common practice in the cost-of-crime literature of including anticipation and response costs in the final tally of the costs of crime. As Levi and Burrows (2008, p. 294) observe, such an inclusion can yield paradoxical results, "if one includes the costs of responses to crime as part of the 'costs of crime,' the less that is done about them, the lower are the 'costs of crime'" and vice versa (see also Dorn & van de Bunt, 2010; Greenfield & Paoli, 2013).

Despite these caveats, the cost-of-crime literature has grown substantially over the past two decades (e.g., Brand & Price, 2000; Cohen et al., 2004; Cohen & Piquero, 2009; Dubourg & Prichard, 2007; Heaton, 2010; Mayhew, 2003; Roman, 2011). In a systematic literature review, Wickramasekera et al.

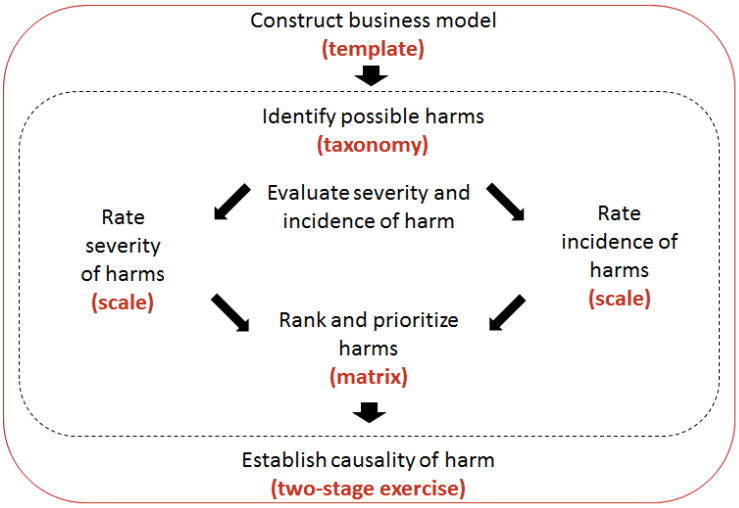
[23] Czabański (2008, pp. 10-17) offers yet another categorization.
[24] As noted below, some studies attempting to measure the costs of cybercrime have defined direct and indirect costs in alternative ways (e.g., Anderson et al. 2013).
[25] Heaton (2010) provides an accessible overview of the main approaches in the cost of crime literature.

(2015) identified twenty-one studies that estimated the cost of crime, concluding that there was a "large variance in the total cost estimates" and that this variance "could be due to changes in unit costs, changes in crime trends, and variations in the methods used to estimate costs". Along these lines, we share Paoli and Greenfield's (2013) assessment that the cost-of-crime literature can provide methodological guidance and insight to direct costs (as defined by Wickramasekera et al., 2015), but it is on much shakier grounds when it attempts to put a price tag on other elements of harm that are not easily amenable to monetization.

1.2.3. The Harms of Crime

Despite the centrality of harm to crime (Paoli & Greenfield, 2017), EU policy-making and law enforcement agencies' recent attempts to set harm-based priorities in crime control (e.g., TFEU, 2008, Art. 83(1); see also Paoli, Adriaenssen, Greenfield & Coninickx, et al., 2016), the empirical, systematic assessment of the harms of crime has long remained a "blind spot" within criminology (see Paoli & Greenfield, 2013). Paoli and Greenfield (2013) could find only three scholarly attempts to categorize the harms of crime — those of Maltz (1990), von Hirsch and Jareborg (1991), and Dorn and van de Bunt (2010). With few exceptions (Clarkson, Cretney, Davis & Shepherd, 1994; Maltz, 1990; Shepherd, 1997), these attempts have not been put to use in empirical assessments.

Figure 1. The harm assessment process



Source: Greenfield & Paoli, 2013.

To fill the gap, Greenfield and Paoli (2013) developed a harm assessment framework. We discuss this framework in some detail, because we have drawn from it our conceptualization of harm. The framework consists of a set of analytical tools woven together in a multistep process that can be used to identify, evaluate, rank, and prioritize harms (see figure 1). One of the tools is a taxonomy that gives practical meaning to "harm" by calling out the potential claimants or "bearers" of harm and the types of harms they might experience in association with each criminal activity under consideration (table 1). The taxonomy accommodates the possibility of harms to each of four general "classes" of bearers that, together, might constitute much of a society, namely: individuals; private-sector entities, including businesses and non-governmental organizations (NGOs); the government; and the social and physical

environment.[26] Bearers in each class experience harms as damages to one or more "interest dimensions" (von Hirsch & Jareborg, 1991), consisting of functional integrity, material support, reputation, and privacy and autonomy. As apparent in table 1, not all interest dimensions pertain to all classes of bearers and damages to a particular dimension, such as functional integrity, can manifest differently across classes. Following von Hirsch and Jareborg (1991), who build on Sen (1987), Greenfield and Paoli (2013) treat these interest dimensions as representing capabilities or pathways to achieving a certain quality of life, referred to as a "standard of living," or, by analogy, institutional mission. The severity of harm depends on the extent to which damages intrude upon either the standard of living or institutional mission; the greater the intrusion, the more severe the harm (von Hirsch & Jareborg, 1991).

Table 1. Bearers and types of harms

Interest dimension	Class of bearer			
	Individuals	Private sector, including businesses and NGOs	Public-sector, including government	Environment, including social and physical
Functional integrity	X[a]	X[b]	X[b]	X[c]
Material support	X	X	X	n/a
Reputation	X	X	X	n/a
Privacy and autonomy	X	X	X	n/a

Note. X = applicable; n/a = not applicable.

a. Functional integrity refers to physical, psychological, and intellectual integrity.

b. Functional integrity refers to operational integrity.

c. Functional integrity refers to physical, operational, and aesthetic integrity

Source: Paoli and Greenfield's (2017) adaptation of Greenfield and Paoli (2013).

Drawing additionally from Greenfield and Camm (2005), the framework ranks harms on the basis of both their severity and incidence (see table 2). At one end of the spectrum, the damage to an interest could be "marginal" and occur only "rarely," at the other end, it could be "catastrophic" and occur "continuously." As shown in Figure 1, Greenfield and Paoli's assessment process begins with the characterization of the criminal activity and ends with an investigation of causality. Absent a specific tool, Greenfield and Paoli (2013) consider causality in two stages. First, they distinguish the harms that result directly from a criminal activity from those that are "remote" and, second, they examine the extent to which they are intrinsic to that activity or arise from the policy environment and related law enforcement practices. Remoteness, in their assessments, refers to the temporal, spatial, or behavioral distance that separates a conduct from its consequences (Greenfield & Paoli, 2013).

[26] Greenfield and Paoli (2013) define 'government' as all state entities (executive, legislative, or judicial), ranging from local to national, but could include supranational and other publically-funded or -managed governing bodies.

Table 2. Matrix for prioritizing harms*, including scales of severity and incidence*

Severity	Incidence				
	Continuously	Persistently	Occasionally	Seldom	Rarely
Catastrophic	VH	H	H	H/M	M/H
Grave	H	H	H/M	M/H	M
Serious	H	H/M	M/H	M	L
Moderate	H/M	M/H	M	L	L
Marginal	M/H	M	L	L	L

Note. VH = Very high priority; H = High priority; M = Medium priority; L = Low priority
Sources: Paoli and Greenfield's (2017) adaptation of Greenfield and Camm (2005, p. 48), drawing from Department of the Army et al. (2001) and other military doctrine, and Paoli et al. (2013).

With different colleagues, Paoli and Greenfield have tested the framework on drug production, drug trafficking, and human trafficking in Belgium and the Netherlands (e.g., Paoli, Zoutendijk & Greenfield, 2013) and demonstrated that it can produce reliable, multi-faceted, and policy-relevant harm "estimates."

1.3. The Impact, Costs and Harms of Cybercrime

In addition to several reports exclusively investigating the incidence of cybercrime (e.g., Europol, 2017), we have identified 15 other studies that assess the negative effects of cyber incidents for businesses. We present an overview of these studies in the first subsection, summarizing their conceptualization of cybercrime and cost, impact or harm in table 3. In the following subsections, we review four of the best and/or most cited/authoritative studies that have attempted to assess the costs and harms of cybercrime via surveys. These are Ponemon's *Cost of Cyber Crime Survey* (2016), PwC's (2016) *Global Economic Crime Survey* and *Information Security Breaches Surveys* (PwC UK, 2015; PwC Belgium; 2017), which have been conducted multiple times as well as the *Cyber Security Breaches Survey* carried by Klahr, Shah, Sheriffs, Rossington, Pestell, Button & Wang (2017) on behalf of the UK government. We conclude the literature review by critically considering two other studies funded by the UK government, which have attempted to assess the impact of cybercrime on the basis of existing data: those of Detica (2011) and Anderson et al. (2013).

1.3.1. A Comparative Overview

Most of the selected studies have been conducted by consulting firms, such as PwC (2016), or businesses selling cybersecurity products, such as McAfee (2014) or Verizon (2016), or private research institutes working on behalf of businesses (e.g., Ponemon, 2016), but a few of the studies have been contributed by academic scholars (e.g., Anderson, 2013; Klahr et al., 2016) mostly on behalf of national governments. Many of the studies carried out by businesses have been repeated at regular intervals, often annually (e.g., those of Ponemon and PwC). Some of these private institutional authors, moreover, publish different studies targeting different geographical areas or different techniques. PwC, for example, has conducted an Information Security Breaches Survey in both the UK and Belgium (PwC Belgium, 2017; PwC UK, 2015), whereas Ponemon has published several studies focusing on specific cyber techniques, (e.g. malware; Ponemon, 2015). In our summary table below, we list only the latest edition of all the different studies that have been carried out more than once.

The studies produced by consulting and security companies are often not explicit about their conceptualization of cybercrime, cost and impact, and their methods of data collection and assessment. They have also been criticized for overestimating – and even artificially inflating – both the incidence as the economic impact of cyber incidents (Anderson et al., 2013; Armin et al., 2016, p. 140; Cashell, Jackson, Jickling & Webel, 2004, p. 3; De Cuyper & Weijters, 2016, p. 16; Wall, 2007, pp. 23-24). Despite their shortcomings, the security and consulting company reports frequently get considerable media attention and thus shape public perceptions about cybercrime (CSI, 2011, p. 9; Wall, 2007, p. 24).

As far as the methodology is concerned, we have catalogued the studies into three groups:

- The first group consists of studies that collect empirical data on the negative effects of cyber incidents on businesses via surveys (e.g., CSI, 2011; Federation of Small Business, 2012; Ponemon, 2015, 2016a, 2016b; PwC Belgium, 2017; PwC UK, 2015; VU Amsterdam & PwC, 2014), in some cases supplementing this quantitative data with in-depth interviews (e.g. CPNI, 2014; Klahr et al., 2017). In this group, we find, both studies conducted by businesses, and academics.
- A second group is produced by private security companies and draws mainly upon user information the companies automatically receive via their products (e.g. McAfee, 2014; Verizon, 2016).
- A third, smaller, group includes studies that analyze information derived from existing data sources (e.g., Anderson et al., 2013). Their authors have so far been exclusively academics.

Each of these types of studies encounters difficulties in determining the real extent of the problem under investigation. The studies collecting data via surveys--by far the most frequent—mostly rely on convenience and/or small samples (e.g., PwC, 2016 and Ponemon, 2016). Their ability to assess the true scale of the problem is also hindered by the businesses' low willingness to report their cybercrime victimization to the outside world (e.g., police, academics, etc.; see Armin et al., 2016, p. 138; CPNI, 2014, p. 4). These two problems—small samples and high refusal rates—are rendered even more problematic by the fact that cybercrime victimization, and particularly the experience of serious harms, are not evenly distributed across the population, with few businesses suffering the most serious harm. (Florêncio & Herley, 2013, pp. 39-43). The social desirability response bias—that is respondents' tendency to answer survey questions in conformity with social expectations—is also likely to be particularly pronounced in surveys about corporate cybercrime victimization. This response bias can be driven by either *impression management* or *self-deception* (Paulhus, 1984; Zerbe & Paulhus, 1987). Impression management refers to deliberately falsifying or manipulating test responses to create favorable impressions (Dutton & Hemphill, 1992; Zerbe & Paulhus, 1987, p. 253), while self-deception refers to an honest, positive self-bias, in which participants actually believe their reports to protect and maintain self-esteem and self-beliefs (Dutton & Hemphill, 1992).

Furthermore, businesses may just as well be simply unaware of their victimization of the severity of its impact (Wall, 2007, p. 20). Klahr et al. (2016, p. 39), for example, report that only five per cent of the 1.000 UK companies they examined had a monitoring system for the financial cost of cyber security incidents in place. For all these reasons, it is thus likely that studies based on surveys lead to an underestimation of the true scale of the issue at stake.

Table 3. Studies investigating the impact/cost and harm of cybercrime on businesses

Study	Conceptualization of cybercrime	Conceptualization of negative effect
Studies primarily based on surveys	*Technology/outcome/mixed/unclear*	

Centre for the Protection of National Infrastructure (2014)	Unclear ("cyber attacks")	Costs (monetized)
		• Costs in anticipation of crime (i.e. security expenditure and insurance administration costs)
		• Costs as consequence of criminal events
		  o Clean-up or remediation costs
		  o Lost user productivity
		  o Disruption of operations
		  o Damage to or theft of IT assets or infrastructure
		  o Damage to reputation or brand value
		  o Damage to competiveness due to stolen intellectual property or commercially sensitive information
		• Costs deriving from the response to crime/costs of enforcement, i.e., costs to the criminal justice system

Computer Security Institute (2011)	Mixed Outcome/offence: examples • Financial fraud • Extortion or blackmail associated with threat of attack or release of stolen data Techniques: examples • Malware infection • Bots/zombies within the organization • System penetration by outsider	Financial losses (i.e., loss of mobile hardware; monetized) • Direct losses, anything attributable to the breach that the business has to write a check for (e.g. responding to incident, hiring forensic investigator and sending out breach notification letters) • Indirect losses, e.g., loss of customers, loss of future business, and loss of capital due to drop in stock price of publicly traded business
Federation of Small Business (2012)	Mixed <u>Online crime:</u>	Costs to businesses (monetized): aggregated figure with no further specification

	• Virus infection • Hacking or electronic intrusion • System security breach in terms of loss of availability • Victim of phishing email • Breach of confidentiality or integrity • Online banking fraud / Account takeover • Other	
Klahr et al. (2017)	Mixed <u>Technique to commit breaches:</u> • Fraudulent emails or being directed to fraudulent websites • Viruses, spyware or malware • Others impersonating the organization in emails or online • Ransomware • Illegal use of computers, networks or servers by outsiders • Hacking or attempted hacking of online bank accounts • Denial-of-service attacks • Illegal use of computer networks • Any other breaches or attacks <u>Outcome of breaches:</u> • Temporary loss of access to files or networks • Software or systems corrupted or damaged • Website or online services taken down or slowed • Lost access to relied-on third-party services • Permanent loss of files (not personal data)) • Money stolen • Personal data altered, destroyed or taken Lost or stolen assets, trade secrets or intellectual property	Impact and costs (monetized): Impact (not defined) on: <u>Recovery time</u> <u>Direct costs:</u> • Staff being prevented from carrying out their work • Lost, damaged or stolen outputs, data, or assets <u>Recovery costs:</u> • Additional staff time needed to deal with the breach or to inform customers or stakeholders • Costs to repair equipment or infrastructure • Any other associated repair costs <u>Long-term costs:</u> • Loss of share value • Loss of investors or funding • Long-term loss of customers • Costs from handling customer complaints • Any compensation, fines or legal costs

Ponemon		

- Cost of Cybercrime (2016)	General: unclear ("criminal activity conducted via the Internet")
	
	Concrete: mixed
	• Stealing intellectual property
	• Confiscating online bank accounts
	• Creating and distributing viruses
	• Posting confidential business information on the Internet
	• (Disrupting a country's critical national infrastructure)
		Costs (monetized)
		
		Total annual cost of cybercrime
		
		Two types of costs
		• "Internal cost activity centers" (cost related to dealing with cybercrime)
		  o Detection costs
		  o Investigation & escalation costs
		  o Containment costs
		  o Recovery costs
		  o Ex-post response costs
		• Costs related to "external consequences of cyber attack"
		  o Information loss or theft
		  o Business disruption
		  o Equipment damage
		  o Revenue loss
		
		Three types of costs (related to dealing with cybercrime?)
		• Direct costs
		• Indirect costs
		• Opportunity costs

- Cost of Data Breaches (2016)	Outcome: data breach	Costs (monetized) of: • Typical activities for discovery and the immediate response to the data breach (e.g., conducting investigations and forensics to determine the root cause of the data breach, conducting communication and public relations outreach) and

		• typical activities conducted in the aftermath of discovering the data breach (e.g., audit and consulting services, identity protection services) The costs resulting from these activities are categorized as: • Direct costs • Indirect costs • Opportunity costs
- Cost of Malware Containment (2015)	Technique: malware or other malicious programs driven threats	Costs: time wasted responding to inaccurate or erroneous malware alerts (non-monetized), translated into monetary estimate per week and year (based upon fully loaded wage hourly rate)
PwC		
- Global Economic Crime Survey (2016)	Unclear (cyber economic crime), two segments identified • Cyber fraud • Transfer-of-wealth/IP attacks or (international) cyber espionage	Losses (total; monetized) Impact (none to high; non-monetized) on: • Reputational damage • Legal, investment and/or enforcement costs • Service disruption • Theft or loss of personal identity information • Regulatory risks • Actual financial loss • IP theft, including theft of data

- UK Information Security Breaches Survey (2015)	Outcome: (security/data) breaches or security incidents
	Types of breaches:
	• Infection by viruses or malicious software
	• Theft or fraud involving computers
	• Other incidents caused by staff
	• Attacks by an illegal outsider (excluding hacking attempts)
		Costs and consequences (worst incident?)
		• (Cyber security investment (percentage of respondents that did this))
		• Monetized
		  ○ Business disruption
		  ○ Time responding to incident

		○ Lost business ○ Direct cash spent responding to incident ○ Regulatory fines and compensation payments ○ Lost assets (including lost intellectual property) ○ Damage to reputation ○ Total (based on previous aspects) • Non-monetized ○ Business disruption (from insignificant to very serious and from none to more than a month; number of days; non-monetized) ○ Time spent to respond to incident (number of man-days) Aspect that made an incident the worst (business disruption, costs to investigate and fix, value of lost assets, reputational damage, other)
- Belgian Information Security Breaches Survey (2017)	Outcome: breaches Techniques as underlying breach vectors • Social engineering/phishing • Regular malware • Human error • Physical theft/loss • C2 malware • Insider breach/privilege abuse • Exploitation of unpatched (known) vulnerability • Stolen credentials • Exploitation of previously unknown vulnerability	(Financial) impact/costs/losses: money lost as result of breach and money spent to responding to incident (monetized; scale going from nothing to more than € 1.000.000, with ranges in between) Aspect that made an incident the worst (business disruption, costs to investigate and fix, value of lost assets, reputational damage, other)

VU Amsterdam & PwC (2014)	Mixed • Cyber espionage • ID theft • Intentional damaging of an IT system • Illegal interception of data • Hacking or hacktivism • Illegal downloads • Viruses • Phishing or pharming	<u>Harms of economic crime, distinguished as ("cybercrime" and not-cybercrime):</u> <u>Harm dimensions:</u> 4-point scale (1-4) • Share price • Relationship with authorities • Business relationships • Reputation • Work ethic • Checks by authorities • Management time
Studies based on automatically collected data		
Center for Strategic and International Studies (2014)	Unclear ("cybercrime", cyberespionage)	"Our estimate looks at both direct costs and indirect costs, and data used that takes into account the loss of intellectual property, the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including reputational damage to the hacked business" (2014, p. 4). Cost presented as % of GDP
Verizon (2016)	Mixed Outcome: • Data breaches Techniques used in order to complete the data breach (sic):	Median records breached by data type (Payment Card Industry Information (PCI), Protected Health Information (PHI), Personally Identifiable Information (PII), Non-card Financial Information)

	• Web App Attacks • Point-of-Sale Intrusions • Insider and Privilege Misuse • Miscellaneous Errors • Physical Theft and Loss • Crimeware • Payment Card Skimmers • Cyber-espionage • Denial-of-Service Attacks • Everything else	
Studies based on secondary data		
Anderson et al. (2013)	General: 2007 EU Commission communication Concrete: mixed • Online payment card fraud • Online banking fraud • In-person payment card fraud • Fake antivirus • Infringing pharmaceuticals • Copyright-infringing software • Copyright-infringing music and video • Stranded traveler scams • Fake escrow scams • Advance fee fraud • PABX fraud • Industrial cyber-espionage and extortion • Fiscal fraud • Other commercial fraud	• Criminal revenue, "the monetary equivalent of the gross receipts from a crime" (p. 269) • Direct losses, "the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime" (p. 270), • Indirect losses, "the monetary equivalents of the losses and opportunity costs imposed on society" (p. 271), • Defence costs, "the monetary equivalent of prevention efforts" (p. 272)
Detica (2011)	Outcome/offence (for businesses) • IP theft	Costs (monetized) • Costs in anticipation of cyber crime

	• Industrial espionage • Customer data-loss • Online theft • Extortion	• Costs as a consequence of cyber crime • Costs in response to cyber crime • Indirect costs associated with cyber crime

Studies based on other data collection techniques also have limitations, though. Those relying on automatically collected data can only give insight on the number of the cyber incidents identified by the security programs. Despite these inherent limitations, the Center for Strategic and International Studies (2014) - working on behalf of McAfee - has managed to develop—on the basis of the cyber breaches reports it receives—an estimate of "both direct costs and indirect cost" as a percentage of GDP. Those relying on secondary data (e.g., Anderson et al., 2013; Detica, 2011) are dependent on the availability of the latter. Whereas Anderson et al. (2013) are transparent about the limitations of this approach, the Detica (2011) has been sharply criticized for providing exaggerated estimates of the costs of cybercrime.

Furthermore, the selected studies have conceptualized cybercrime in a myriad of different ways. Some studies conceptualize cybercrime in terms of specific techniques (e.g., Ponemon's cost of malware study, 2015), thus disregarding the legal definitions of cybercrime offences. Other studies, instead, are technology-neutral and focus on the activities formally defined as offences (e.g., cyber extortion, cyber espionage, illegal access to IT systems etc.), or at least on the final outcome of the activities (e.g., data breach), with no regard for the technique used (e.g., Detica, 2011; Ponemon's cost of data breaches study, 2016b). A third group mixes the two approaches, thus including both techniques and offences/outcomes in their conceptualization of cybercrime (e.g. CSI, 2011; Federation of Small Businesses, 2012; Klahr et al., 2017; VU Amsterdam & PwC, 2014).

Most studies consider the negative effects of cyber incidents for the companies in terms of costs or (financial) losses (e.g., CPNI, 2014; CSI, 2011; Detica, 2011; Federation of Small Businesses, 2012; Klahr et al., 2017; Center for Strategic and International Studies, 2014; PwC, 2015). Some of these studies (i.e., Klahr et al., 2017 and PwC, 2016) also include questions about the impact of cybercrime. These questions are meant to cover the harms of crime that cannot be easily monetized or to introduce more specific questions on the costs of cybercrime. Hence, for example, Klahr et al. (2017, pp. 43-44) ask the respondents to consider which impact the reported breaches (e.g., the loss of access to files or networks, possible downtime of the business's website or the alteration or destruction of personal data) have had on the organization. Respondents can choose items out of a long list, including new measures needed for future attacks, loss of revenue, the added staff time to handle the incident, the disrupted provision of goods and services to customers, complaints from customers and reputational damage, fines or legal costs. Respondents are subsequently asked to indicate the time taken to recover from the most disruptive breach of the last 12 months. Along similar lines, PwC (2016b) asks its respondents to rate on a four-point scale from none to high the impact of cybercrime on reputational damage, legal, investment and/or enforcement costs, service disruption, theft or loss of personal identity information, regulatory risks, actual financial loss and IP theft, including theft of data. In the cybercrime literature, we have identified only one study that uses the term harm to conceptualize the negative effects of cyber incidents: VU Amsterdam and PwC (2014).

The conceptualization of the costs and/or losses also differs from study to study. Some studies simply speak of cost in general with no further operationalization (e.g., Federation of Small Businesses, 2012), while others make a distinction between different types of costs. In compliance with the general cost-of-crime literature, several studies distinguish between direct and indirect costs and/or losses. The Computer Security Institute, (2011), for example, defines direct losses as those for which the business has to write a check for (e.g. responding to incident, hiring forensic investigator and sending out breach notification letters) and indirect losses are those that derive from loss of customers, loss of future business, and loss of capital due to drop in stock price of publicly traded business. Other studies also

refer to the standard distinction in economics between direct and indirect costs, but then do not follow up precisely on their operationalization (e.g., Ponemon, 2016).

Most studies exclusively consider the costs of cybercrime itself and its immediate reaction costs (e.g., Computer Security Institute, 2011; Klahr et al. 2017; Ponemon, 2016). Other studies also attempt to estimate the prevention costs: some of these (e.g., Anderson et al., 2013) keep prevention costs separate from the costs of cybercrime and contrast them with the latter. Other studies (e.g., Centre for the Protection of National Infrastructure, 2014 and Center for Strategic and International Studies, 2014), instead, provide an overall estimate of all costs, lumping together the costs of cybercrime, with those of prevention and even law enforcement costs, thus unsurprisingly depicting dramatically high estimates.

1.3.2. Ponemon's (2016) Cost of Cyber Crime Survey

Since 2009, Ponemon, a US research institute sponsored by companies like HP and IBM, has been annually publishing "Cost of cybercrime" studies. For the first five years, it collected data only among large-scale US businesses. From 2012 onwards, the study has been extended to include the United Kingdom, Germany, Australia and Japan, and since 2015, to Brazil.

Ponemon defines cybercrime as "criminal activity conducted via the Internet." In its introduction, it states that this category also includes "stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country's critical national infrastructure" (2016a, p. 1). The latter category is not mentioned in the further analysis and is, indeed, rather surprising, as Ponemon exclusively collects data on the costs suffered by businesses. Later in the report, Ponemon includes other classifications consisting of malware, phishing, SE (social engineering), web-based attacks, malicious code, botnets, stolen devices, denial of services and malicious insiders. It provides no definition of these subcategories, although some of them can be overlapping (e.g., malware, web-based attacks, malicious code, botnets). In a footnote, Ponemon (2016a, p. 30) acknowledges that "these nine attack categories are not mutually independent and they do not represent an exhaustive list. Classification of a given attack was made by the researcher and derived from the facts collected during the benchmarking process."

Ponemon divides the costs of cybercrime in two major categories (see figure 2):

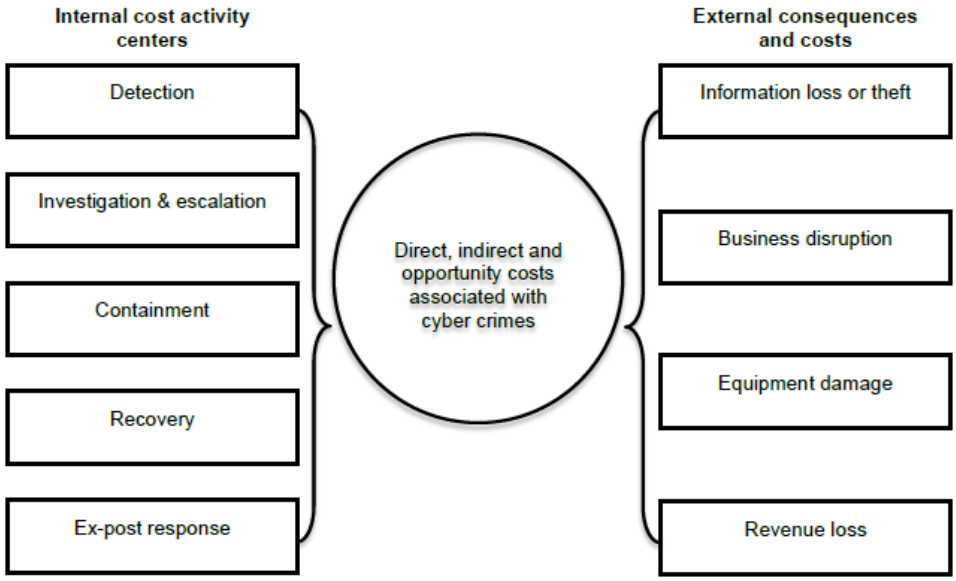
- The so-called "internal cost activity centers", that is, the costs related to dealing with the cybercrime (mainly, but as explained below, not exclusively, personnel costs), and
- "The external consequences of the cyberattack", a category that includes inform loss of theft, business disruption, equipment damage and revenue loss (2016a, p. 29).

For the first category, Ponemon writes that it analyzes the internal cost centers sequentially—starting with the detection of the incident and ending with the ex-post or final response to the incident. This latter phase is said to also include dealing with lost business opportunities and business disruption, which are also part of the second category. Ponemon also introduces the distinction between direct costs, indirect costs and opportunity costs (2016a, p. 29), but it does not use this distinction in its analyses. It explicitly excludes general prevention and compliance costs defined as "the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations" (Ponemon, 2016a, p. 28).

To measure the internal cost centers and external consequences of the cyberattack, Ponemon does not administer surveys, rather it conducts interviews with a small number of large-scale businesses in the selected countries. In the first US studies, Ponemon selected 50 businesses. The sample has since then grown to 237 businesses. However, since the number of selected countries has grown to six, this means that less than 40 businesses are interviewed per country. Ponemon does not provide the number of selected businesses per country. Despite these small figures, Ponemon (2016a, p. 1 and p. 35) claims that its sample is "representative." In the final page of the report, it admits, though, that "non-response bias was not tested, which means that it Is possible that companies that did not participate are substantially different in terms of the methods used to manage the cybercrime containment and recovery process, as well as the underlying costs involved."

At each business, Ponemon conducts multiple interviews with senior-level personnel, but the exact number of them is unclear: in the 2016 report it writes that it conducted 1,278 interviews (p. 1), while in the methodology section it reports 2,050 interviews (p. 31).

Figure 2. Ponemon's framework of cybercrime costs



Source: Ponemon, 2016, p. 28.

To determine the average cost of cybercrime, the selected businesses are asked to report what they spent to deal with the cybercrimes experienced over four consecutive weeks. Ponemon notes, though, that its "cost method does not require subjects to provide actual accounting results" (2016a, p. 31). For both categories of costs, the estimation process apparently works in two steps. First, in a benchmarking process, the interviewees rate for each subcategory of costs, their "best estimate for the sum of cash outlays, labor and overhead incurred" and, separately, for their "indirect and opportunity costs" along a line ranging from a lower and an upper limit (2016a, p. 31). In a second step, Ponemon compiles cost estimates for each business "based on the relative magnitude of these costs in comparison to a direct cost within a given category" and it estimates revenue losses on the basis of "general interview questions to obtain additional facts" (2016a, p. 32). Ponemon writes that that it captures revenue losses, business disruption and other external costs "using shadow-costing methods," but it does not elaborate

on how this is done. Later, it admits that "the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results" (2016a, p. 35).

Ponemon does not specify if it estimates the costs for each cybercrime episode occurred during the four-week period, or for the total or an average of them. Once costs over the four-week period are compiled, it aggregates these figures to determine the annualized cost.

In its 2016 report, Ponemon states that each business suffered on average of two attacks per week (p. 8). The median annualized cost of cybercrime is $6.7 million and the mean value is $9.5 million. These figures represent increases of 22 and 21 percent, respectively in comparison with the 2015 values (p. 5). US businesses continue to have the highest average cost of cybercrime ($17.36 million), and Australia has the lowest ($4.30 million; p. 4). In 2016, the highest annualized costs were experienced by businesses in financial services and utilities & energy experienced (p. 7).

Ponemon does not provides an estimate of the costs for each type of cybercrime, nor does it clarify the relative weight of internal and external costs. It only claims that "information loss or theft is now the most expensive consequence of a cybercrime," but then presents only the percent weight of this and other external costs within the category of external consequences, with information loss at 39%, business disruption at 36%, and revenue loss at 20%.

Over half of the report describes the businesses' current security investments and the necessary security capabilities and applications. Ponemon emphatically stresses "the good news" that a high security profile decreases the cost of cybercrime—even for highly innovative companies"—a message that its sponsor, HP, is most probably very eager to hear (2016a, p. 5).

1.3.3. PwC's (2016) Global Economic Survey and Information Security Breaches Surveys (PwC UK, 2015; PwC Belgium, 2017)

PwC carries out a Global Economic Crime Survey (GECS), a worldwide survey on economic (business) crime and its costs, every two years. In 2016, the survey also included cybercrime, considering it a specific type of economic crime. In the report of this survey, PwC argues that "cyber economic crime has evolved to a point where one could segment it into two distinct categories – the kind that steal money and bruise reputations and the kind that steal IP and lays waste to an entire business", referring to cyber fraud on the one hand and (international) cyber espionage on the other hand (PwC, 2016, p. 19). More concretely, PwC describes cyber fraud as "monetisable cybercrime, such as identity and payment card theft". Cyber espionage, on the other hand, is defined as "the theft of critical IP – trade secrets, product information, negotiating strategies and the like" (PwC, 2016, p. 19).

With regards to the negative consequences of cybercrime, the last round of GECS asks the respondents two questions. First, they asked the respondent to indicate the total amount of money the organization had lost due to all cybercrime incidents in the past two years (on a 7-point scale ranging from *no loss* to *100 million USD or more*). Second, the respondents are invited to rate on a 4-point scale, ranging from *none* to *high*, the impact cybercrime has had on the following aspects of their business: reputational damage; actual financial loss; legal, investment and/or enforcement costs; regulatory risks; service disruption; IP theft, including the theft of data; and theft or loss of personal identity information (PwC, 2016, p. 18). This is a good solution that helps account for the harm that cannot be easily monetized. However, the list of the impacted items includes two types of cybercrimes (i.e., IP theft, including the theft of data, and theft or loss of personal identity information), thus making the question about the

impact circular. These problems lead us to conclude that the GECS does not make a clear conceptual distinction between cybercrime and its impact. There also seems to be no clear distinction between cost and impact, as the category of impact includes "legal, investment and/or enforcement costs."

The operationalization of cost also seems to be deficient. The GECS does not ask how many resources were necessary to respond to cybercrime, but only how much money the business has lost as a result of all cyber incidents in the past two years. It seems unlikely that most businesses are able to answer with any precision this question. In addition to these issues of conceptualization, there are also some methodological issues. PwC, for example, reports that 6.337 business representatives, spread over 115 different countries, completed the GECS in 2016, but it does not provide detailed information on the geographical distribution of the survey respondents across all countries. In some countries, the number of respondents is insufficient to draw conclusions specifically for each of those countries (e.g., only 58 respondents in Belgium, PwC Belgium, 2016).

As for the results, the latest GECS (PwC, 2016) reports that a quarter of the respondents have been affected by cybercrime. Approximately a quarter of the victimized companies indicated that they had not suffered losses as a result of the incidents. One third reported losses below 50.000 USD, 12% losses between 50.000 USD and 100.000 USD and 16% losses over 100.000 USD[27]. With regards to impact, the respondents considered reputational damage "the most damaging impact of a cyber breach", followed by legal, investment and/or enforcement costs (p. 19). However, this assertion is not entirely supported by the data, which shows only small differences between the impact on the different aspects (cf. supra).

In addition to the GECS, PwC UK has run the Information Security Breaches Survey (ISBS), since the 1990s. Some years ago, PwC Belgium also started with an ISBS. In both the UK and Belgium, the ISBS is country-specific and dedicated solely to data or security breaches and the costs these breaches produce. However, in both cases, such data or security breaches are not clearly conceptualized. The report of the latest Belgian ISBS identifies only some *underlying breach vectors* (e.g. phishing, malware, human error, etc.; PwC Belgium, 2017, p. 7), while the latest UK ISBS identifies only some *types* of breaches (infection by viruses or malicious software; theft or fraud involving computers; other incidents caused by staff; attacks by an illegal outsider; PwC UK, 2015, p. 11). As evident in the examples provided, there are some similarities between the breach vectors identified in the Belgian ISBS, and the types of breach identified in the UK ISBS.

Furthermore, both ISBSs look at the impact of incidents. In the Belgian ISBS, the focus is on the direct financial losses, i.e. the amount of money lost as a result of an incidents and the money spent to respond to an incident. This survey also contains a question in which the respondents are asked to indicate which of the aspects of business disruption, investigation and fixing costs, value of the lost assets or reputational damage rendered a specific incident the worst of the year. The UK ISBS adopts a similar approach, but also tries to monetize the impact on business disruption, response time, lost business, direct cash spent responding to incident, lost assets and reputation damage (for the worst incident; PwC UK, 2015, pp. 21-23). Combining all those estimates, they try to estimate the total cost of the (worst) incident.

[27] 15% of the respondents did not know how much their company had lost as a result of cyber incidents in the past two years.

In 2015, 664 people completed the UK ISBS (PwC UK, p. 5), but the sample size for some items was much lower. The last ISBS in Belgium involved only 98 respondents.

In the latest UK ISBS, we see that 90% of the large businesses, and 74% of the small businesses in the sample, experienced a security breach in the past year, with a median number of breaches of 14 for large businesses, and four for small businesses. In the Belgian ISBS, no total percentages were given for victimization of breaches, let alone split up for large and small businesses. It was only stated that 15% had suffered from a "serious breach." In latest UK ISBS report, the percentages of victimization of a "serious incident" were much higher (66% for large businesses and 25% for small businesses). However, it is not clear whether the conceptualization of serious breaches (in the Belgian ISBS; PwC Belgium, 2017) and serious incidents (in the UK ISBS; PwC UK, 2015) are the same.

With regards to costs, 21% of the Belgian respondents indicate that they did not have direct financial losses as result of a breach; 47% had direct financial losses, and 32% did not know whether they had had financial losses as result of a breach. Furthermore, 5% indicate that they spent no money on incident response; 63% spent money on incident response, and 32% did know how much they had spent on incidence response. On the other hand, the report of the latest UK ISBS, describes the range of the average total costs incurred from the worst security incident suffered by the respondents. These costs ranged from £75.000 to £311.000 for small business, and from £1.46 million to £3.14 million, for large businesses. Such high amounts are attributable to the generous conceptualization of costs. These estimates are also characterized by huge ranges, thus suggesting that there are enormous differences in impact of different cybercrimes on businesses. Finally, looking at what made an incident the worst of the year, we see that the costs to investigate and fix the breach were ranked first in the Belgian ISBS, followed by reputational damage and the rest category of other. In the UK ISBS, reputational damage is ranked first, followed by business disruption (only ranked fourth in Belgian ISBS) and costs to investigate, or fix.

1.3.4. Klahr et al. (2017)'s Cyber Security Breaches Survey

Since 2016, researchers of the University of Portsmouth and Ipsos MORI (Klahr, Shah, Sheriffs, Rossington, Pestell, Button & Wang, 2017) conduct an annual *Cyber security breaches survey* on behalf of the UK Government. The UK Government uses this survey to support businesses in their cyber security efforts, and to make informed policy decisions. In order to achieve this aim, Klahr et al.,for the 2017 report, administered a telephone survey to a random sample of 1,523 UK businesses[28], and subsequently conducted in-depth interviews with representatives from 30 businesses. Thanks to this random sampling, and the weighing of the survey data, they assert that their study is representative for businesses belonging to 11 economic sectors (Klahr et al., 2017, p. 4-5).[29]

In addition to questions about businesses' attitudes towards cyber security, the survey investigates the cybercrime victimization experiences of the selected businesses, including the related impact and costs. First, businesses are asked whether they were victim of a cyber security breach or attack in the last 12 months (Klahr et al., 2017, p. 39). The survey covers nine types of incidents:

[28] Only businesses with an IT capacity or online presence were eligible for the survey.

[29] 'Administration or real estate', 'Construction', 'Education, health or social care', 'Entertainment', 'Finance or insurance', 'Food or hospitality', 'Information, communications or utilities', 'Manufacturing', 'Professional, scientific or technical', 'Retail or wholesale' and 'Transport or storage'.

- “Fraudulent emails or being directed to fraudulent websites,”
- “Viruses, spyware or malware,”
- “Others impersonating organization in emails or online,”
- “Ransomware,”
- “Illegal use of computers, networks or servers by outsiders,”
- “Hacking or attempted hacking of online bank accounts,”
- “Denial-of-service attacks,”
- “Unauthorised use of computers, networks or servers by staff,” and
- The residual category, “any other breaches or attacks” (Klahr, 2017, p. 41).

This typology can be praised for its exhaustiveness. However, it is not technology-neutral since it includes specific techniques that can be deployed to commit different offences. Ransomware and denial-of-service attacks, for example, are techniques that induce interferences, but can also be used to commit further offences, for example, to extort.

In addition to the victimization rate, and the single breach, or attack, that caused most disruption to the business, Klahr et al. (2017, pp. 43-44) asked the respondents to describe the outcomes resulting of all the cyber security breaches or attacks experienced in the last 12 months (e.g., the loss of access to files or networks, possible downtime of the business’s website or the alteration or destruction of personal data). Then they asked them to consider which impact any of these breaches have had on the organization. Respondents could choose items out of a long list, including new measures needed for future attacks, loss of revenue, the added staff time to handle the incident, the disrupted provision of goods and services to customers, complaints from customers and reputational damage, fines or legal costs. In a third step, respondents had to indicate the time needed to recover from the most disruptive breach of the last 12 months. Fourth, they were asked to estimate “the costs … businesses have incurred from all the cybersecurity breaches they have experienced in the past 12 months, taking into account all impacts they mentioned resulting from these breaches” (Klahr et al. 2017, p. 46). Klahr et al. (2017, p. 46) admit that “it is very uncommon for businesses to monitor the financial costs of cyber security breaches,“ but still ask their respondents to estimate “direct costs,” “recovery costs” and “long-term costs” (Klahr et al., 2017, p. 47).

To estimate these three categories of costs, they group all the possible impacts into these three categories and ask the respondents to place a general monetary value on each of them. Direct costs include “costs from staff being prevented from carrying out their work; lost, damaged or stolen outputs, data, or assets; and lost revenue if customers could not access online services” (Klahr et al., 2017, p. 47). Recovery costs include “additional staff time needed to deal with the breach or to inform customers or stakeholders, costs to repair equipment or infrastructure and a remaining category that groups “any other associated repair costs” (Klahr et al., 2017, p. 47). Finally, long-term costs are understood as “loss of share value, loss of investors or funding, long-term loss of customers, (costs from handling customer complaints’ and “any compensation, fines or legal costs.” With regard to the latter category, the authors note that these types of costs are more difficult to estimate, resulting in higher margins of error in the respective figures (Klahr et al., 2017, p. 48). Lastly, the respondents are asked to reassess the three cost items as mentioned above, but this time with respect to the one cyber security breach, or attack, that caused the most disruption to the organization.

As for the results, just under half of the of the businesses report to have suffered at least one cyber security breach in the last year. The frequency of the incidents is related to the business size (Klahr et al., 2017, p. 39). Among the types of cybercrime reported, receiving fraudulent emails, or being directed to fraudulent websites, tops the list (72%), followed by, getting infected with viruses; spyware and malware (33%); others impersonating the organization in emails or online (27%); ransomware attacks (17%), and the illegal use of computers, networks, or servers by outsiders (10%) (Klahr et al., 2017, p. 41). Almost 60% of the businesses indicate that the breach had no significant impact. Twenty-three percent, however, mention that the breach resulted in the temporary loss of access to files or networks; 20% admit that their software or systems were corrupted or damaged, and 9% indicate that their website or online services were taken down or slowed in the wake of the breach (Klahr et al., 2017, p. 43).

Interestingly, the median cost of all breaches is zero, which highlights that most breaches do not lead to financial losses. The median costs of all three debit entries (direct costs, recovery costs and long-term costs) of the most disruptive breach also equals zero, indicating that even these breaches usually do not lead to financial losses. However, some businesses directly affected by a serious breach can incur substantial financial losses, with the loss again increasing as the firm size does too. When looking at the mean direct cost of the most disruptive breach, one sees for example that businesses with less than 50 employees report a mean loss of approximately £1,220, while the mean loss of businesses with more than 250 employees amounts to approximately £4,270 (Klahr et al., 2017, p. 47). A comparable finding can be observed when looking at the mean recovery costs of the most serious breach. This average cost is about £650 for small businesses, while large businesses make reference of an average recovery cost as high as £12,200 (Klahr et al., 2017, p. 48).

1.3.5. Detica's (2011) The Cost of Cybercrime

The Detica (2011) study assessed the costs of cybercrime for the United Kingdom (UK) on behalf of the UK Cabinet Office; the study used four categories:

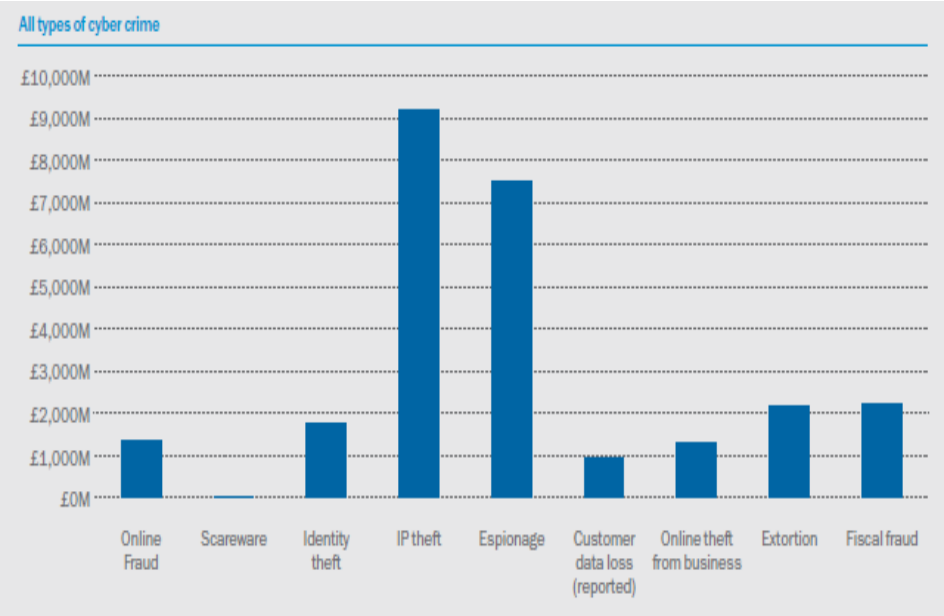
1. costs in anticipation of cybercrime, such as antivirus software, insurance and compliance;
2. costs as a consequence of cybercrime, such as direct losses and indirect costs such as weakened competitiveness as a result of intellectual property compromise;
3. costs in response to cybercrime, such as compensation payments to victims and fines paid to regulatory bodies;
4. indirect costs such as reputational damage to businesses, loss of confidence in cyber transactions by individuals and businesses, reduced public-sector revenues and the growth of the underground economy.

Detica attempted to estimate these costs for a broad set of computer-integrity and computer assisted crimes including identity theft, online scams, scareware, fiscal fraud, theft from business, extortion, customer data loss, industrial espionage, intellectual property (IP) theft, and money laundering. Ultimately, it concluded that in the most likely scenario, the cost of cybercrime to the UK was £27bn per annum (about 1.8% of GDP; see figure 3). A significant proportion of this cost supposedly came from the theft of IP from UK businesses, which they estimated at £9.2bn per annum. UK businesses were seen as the main bearers of the costs, as they experienced costs of £21bn. Detica (2011, p. 2) and, by extension the UK Cabinet Office, claimed that "in all probability, and in line with our worst-case scenarios, the real impact of cybercrime is likely to be much greater."

As Ross Anderson from the Cambridge University Computer Laboratory and his colleagues (2013, p. 267) noted "the Detica report was greeted with widespread scepticism and seen as an attempt to talk up the threat", not least because Detica is a British Aerospace subsidiary and sells data protection and information assurance products. Cybersecurity expert Peter Sommer, for example, was quoted saying that "the report is full of fake precision, with elaborate charts claiming to show the relative costs of IP theft and industrial espionage per industry sector … But we have no means of measuring either in terms of events and no agreement about what to include in losses — how do you calculate a lost business opportunity?" (Espiner, 2011).

In a blog of the Cambridge University Computer Laboratory, one of Anderson's co-authors, Tyler Moore (2011) further argued that "much of the total cost is based on questionable calculations that are impossible for outsiders to verify" (see also Kobie, 2013).

Figure 3. Costs of different types of cybercrime according to the Detica (2011) study



Anderson et al. (2013) in particular, dismissed the Detica's dramatic estimate of IP theft as having "no obvious foundation" and further criticized the study on conceptual grounds, because Detica's second subcategory of cybercrime costs in the latter study mix up both direct and indirect costs.

1.3.6. Anderson et al. (2013)'s Measuring the Cost of Cybercrime

Anderson et al. (2013) produced their own estimate of the costs of cybercrime at the invitation of the UK Ministry of Defense. They adapted the conceptual framework of the Detica study, splitting between direct cost and indirect costs. Figure 4 gives a representation of their conceptual framework.

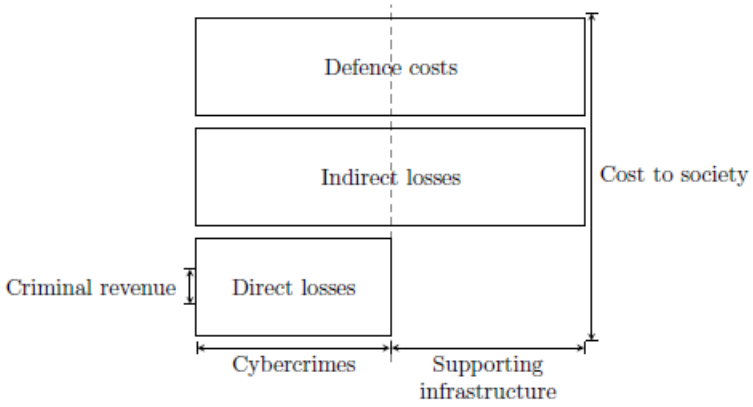
Their main categories consisted of:

- Criminal revenue, that is, "the monetary equivalent of the gross receipts from a crime" (p. 269); here they rightly point out that revenues can be much smaller than the losses incurred.
- Direct losses, that is, "the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime" (p. 270), including money withdrawn from victim accounts; time and effort to reset account credentials (for both banks and consumers); distress suffered by victims; secondary costs of overdrawn accounts, such as deferred purchases; inconvenience of not having access to money when needed; lost attention and bandwidth caused by spam messages, even if they are not reacted to.

- Indirect losses, that is, "the monetary equivalents of the losses and opportunity costs imposed on society" (p. 271), rather than the individual victims, by all attempted and completed cybercrimes. In Anderson et al.'s (2013) view, indirect losses, among others, include loss of trust in online banking, leading to reduced revenues from electronic transaction fees, higher costs for maintaining branch staff and cheque clearing facilities, and even efforts to clean-up PCs infected with the malware for a spam sending botnet. Anderson et al. (2013) further argue that indirect losses arise not only from concrete cybercrimes, but also from their supporting infrastructure, such as botnets.
- Defence costs: these are defined as "the monetary equivalent of prevention efforts" (p. 272) and further distinguished between "direct defence costs, i.e., the cost of development, deployment, and maintenance of prevention measures, as well as indirect defence costs, such as inconvenience and opportunity costs caused by the prevention measures." However, the examples that Anderson et al. provide also include "fraud detection, tracking", "recuperation efforts," and "law enforcement", thus not only prevention but also reaction and repression costs.

Early in their article, Anderson et al. (2013) stress that, as opposed to the Detica (2011) study, they clearly distinguish direct and indirect costs on the grounds that the former can at least be measured accurately, whereas the latter are harder to assess. However, as apparent from their own descriptions, they also mix up direct, direct and intangible costs. For example, the category of direct losses includes "the inconvenience of not having access to money when needed" (p. 270). Moreover, they also seem to mix up indirect losses and defence costs, as "the inconvenience of missing an important message falsely classified as spam" (p. 272) is presented as example of the latter.

Figure 4. Framework for analyzing the costs of cybercrime according to Anderson et al. (2013)



Source: Anderson et al., 2013, p. 270

Subsequently, they apply this conceptual framework to an eclectic list of cybercrimes, primarily consisting of frauds, but also including fake antivirus programs; the online sale of counterfeit or patent-infringing pharmaceuticals and the sales of copyright-infringing software, as well as music and video (see table 3). They also attempt to separately estimate the costs of the infrastructure supporting cybercrime, such as botnets, on the ground that botnets "are used to enable lots of different crimes" and in such a way to avoid double counting. The list seems to be driven by data availability rather than any official definition or academic conceptualization of cybercrime. Disregarding the frequent

distinction between computer-integrity and computer-assisted crime, as well as the tripartite categorization of cybercrime put forward by the European Commission (2007), which they themselves quote, they distinguish four categories: “genuine cybercrime”, “transitional cybercrime”, “traditional cybercriminal infrastructure” and “traditional crimes becoming cyber.” In the first category many types of fraud are included, despite the fact that these constitute a computer-assisted, rather than a computer-integrity crime.

Anderson et al. (2013) provide no estimate of the extent or cost of industrial cyber-espionage and extortion, because “there is no reliable evidence” (p. 286). They also do not provide total figures for each category, arguing that “it is entirely misleading to provide totals lest they be quoted out of context, without all the caveats and cautions that we have provided.”

Anderson et al.’s (2013) conclusions can be summarized as follows:

- The largest harm arises from traditional frauds, such as tax and welfare fraud, which cost each of us as citizens a few hundred pounds/euros/dollars a year and is inversely proportional to the money invested in defense.
- Transitional frauds such as payment card fraud cost each UK citizen a few tens of pounds/euros/dollars a year, with defence costs broadly comparable with actual losses. Here, the authors emphasize the indirect costs of business foregone because of the fear of fraud, both by consumers and by merchants, are several times higher.
- New cyber-frauds such as fake antivirus, generate so far only limited direct losses, but the indirect costs and defence costs are very substantial.

From this data, they draw the final policy implication that “we should perhaps spend less in anticipation of computer crime (on antivirus, firewalls etc.), but we should certainly spend an awful lot more on catching and punishing the perpetrators” (p. 297).

2. Our Conceptualization of the Key Concepts

This chapter presents our definitions of the main concepts of the study, namely "cybercrime" as well as "impact," "harms" and "costs" (of cybercrime), along with our justifications for our choices.

2.1. Cybercrime

Following the approach adopted by legal texts, policy documents and other studies (e.g., UNODC, 2013), the present project does not define cybercrime per se, but rather identifies specific acts that constitute cybercrime. Specifically, and unlike most other studies on the cost and impact of cybercrime, we have developed a "technology-neutral" typology of cybercrime, i.e., a typology that is independent of the specific techniques used by cybercriminals. The typology largely draws from the Council of Europe's Convention on Cybercrime, and the Belgian criminal law concerning cybercrime,[30] but also incorporates the insights from the academic literature on the topic. It consists of five types of cybercrime that may potentially target businesses:

A. Illegal access to IT systems

B. Corporate espionage

C. Data or system interference

D. Cyber extortion

E. Internet fraud.

The first three types belong to the category of "computer-integrity crimes" (Gordon & Ford, 2006, p. 14) and the latter two to the category of "computer-assisted crimes" *(*Wall, 2007, p. 50). Our conceptualization of the three computer-integrity crimes is based upon the Council of Europe's Convention and Belgian cybercrime law. In fact, the incidents of illegal access to IT systems, corporate espionage and data/system interference, correspond, respectively, to the offences of "illegal access" (art. 2), "illegal interference" (art. 4) and "data" and "system interference" (art. 5-6) in the Convention.[31] The type "cyber extortion" has no direct correspondence in the Convention; it is rather the cyber version of a standard offence in Belgian and other national criminal laws. The last type, "internet fraud," draws from the offence of computer-related fraud defined by the Convention (Council of Europe, 2001: 6; art. 8) as well as two other more traditional types of fraud that frequently target businesses online.

2.1.1 Incidents of Illegal Access to IT Systems

This first type is comprised of illegal access to IT systems. The generic term "IT system" exemplifies the technology-neutral way in which the survey is drafted. Following the Council of Europe's 2001 convention, an IT system is conceived as "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".[32] [33]

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

[31] We foresee no pendant for the last computer-integrity crime introduced by the Council of Europe's Convention, i.e., „misuse of device", because this is a preparatory offence for the commission of the other four cybercrime offences.

[32] Art. 1, a, Convention on Cybercrime, Council of Europe, Budapest, November 23th 2001, *E.T.S.*, nr. 185.

[33] This conceptualization of an 'IT system' is maintained throughout the rest of the study.

Illegal access to an IT system can be achieved in many different ways, for example through the use of hackertools, such as exploit kits, Trojan horses, backdoors, password sniffers and the like (e.g., Bernaards et al., 2012, pp. 27-34; ENISA, 2016a, pp. 19-21). In addition, cybercriminals can also avail themselves of specific techniques in order to "socially engineer" log-in information out of unsuspecting users. Supporting techniques include (spear)phishing, password guessing or even checking discarded documents retrieved from the waste disposal (e.g., Bernaards et al., 2012; Leukfeldt, Domenie & Stol, 2009; Van der Hulst & Neve, 2008; Wall, 2007). The Council of Europe's 2001 Convention also compels the parties to criminalize acts of legitimate users of the IT system (e.g., employees, hired consultants etc.) who exceed their access privileges, considering them as instances of illegal access.[34] Illegal access can also occur by exploiting known vulnerabilities in the security – ranging from zero-day vulnerabilities to accessing an unprotected WiFi-network of a business (e.g., Centraal Planbureau, 2016; Verizon, 2016).

This type of cybercrime is often a preliminary step in the commission of more serious cyber offences, such as corporate espionage.

2.1.2 Corporate Espionage

Corporate espionage presupposes illegal access to an IT system (Verizon, 2016, p. 52), regardless of the technique employed. The close link between the two types was also acknowledged by the Belgian criminal (cyber) act of 2000: the Belgian legislator, in fact, has criminalized this offence, by simply adding an extra paragraph[35] to the article concerning illegal access to an IT system. When the espionage attempt is successful, this results in the theft of confidential and protected information that for one reason or another is important for the business (ENISA, 2016a, p. 39). Just as was the case with the conceptualization of an "IT system," our conceptualization of "data" also has a technology-neutral character. Following the Council of Europe's 2001 convention, data is understood here as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."[36]

Corporate espionage is nowadays a common cybercrime (e.g., Europol, 2016; Gemalto, 2016). Several types of data can be targeted, but they all have in common that they are in one way or another of high value to motivated cybercriminals, whether these are malicious insiders, or outsiders, hacktivists, or hostile nation states (Europol, 2016, p. 36; Gemalto, 2016, p. 6; Wall, 2007, pp. 94-101). According to ENISA (2016a, p. 39) identity information is the most frequently targeted and breached type of data (50%), followed by, financial access credentials (over 20%), confidential data, or data on intellectual property (over 10%), and user credentials (over 10%).

Given the great variety of datatypes stored in the IT systems of businesses in different sectors, we have used generic categories for the data that might constitute the primary object of the attack. This includes a) bulk business data (e.g., details of customers or employees and financial details of the organization); b) data on high-value intellectual property (e.g., R&D outputs and product prototypes); c) data containing tactical corporate information (e.g., contract bid prices and documents describing business

[34] Art. 550*bis*, §2 Sw.
[35] Art. 550*bis*, §3, 1° Sw.
[36] Art. 1, b, Convention on Cybercrime, Council of Europe, Budapest, November 23th 2001, *E.T.S.*, nr. 185.

processes or strategies), and d) the residual category "other" (see Detica, 2011, p. 9 and Deloitte, 2016, p. 12).

2.1.3 Data/system interference

The third type of computer-integrity crimes consists of data or system interference. This can be achieved through a myriad of specific techniques (e.g., viruses, worms, cryptoware, (D)Dos-attacks performed by botnets etc.; e.g., Bernaards et al., 2012; Leukfeldt et al., 2009; Van der Hulst & Neve, 2008) but can be classified under two broad categories: data interference (e.g., Van der Hulst & Neve, 2008, pp. 71-73) and system interference (e.g., Van der Hulst & Neve, 2008, pp. 73-77). Both categories are criminalized under Belgian IT law by means of an article referring to the offence of IT sabotage.[37]

In line with the Council of Europe's 2001 convention, an interference - as defined in this study - refers to the intentional "damaging, deletion, deterioration, alteration or suppression of computer data without right"[38] and/or to the "serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data".[39] In practice, most interferences are provoked by malware infections, but they can also result from malicious actions of persons or groups that first gained illegal access to the IT system. Data interferences are mainly caused by (i.e., Distributed denial-of-service) attacks or by spamming. In both cases, the IT system becomes overloaded by the massive quantity of data (requests) sent (Van der Hulst & Neve, 2008, p. 19). In the case of data interferences, the negative impact can vary heavily depending on both their intensity and duration (Centraal Planbureau, 2016, p. 49).

2.1.4 Cyber Extortion

Over the last few years, the number of companies victimized by ransomware has been on the rise drastically (ENISA, 2016a, p. 45; Europol, 2016, p. 17; Munnichs, Kouw & Kool, 2017, p. 15; Van Leiden, Appelmann, Van Ham & Ferwerda, 2014, p. 41). A system can become infected with this type of "crimeware" through multiple techniques, ranging from infected email attachments or links to other types of malware. (Domenie et al., 2013, p. 39; Verizon, 2016, p. 46). The malware encrypts data stored in the IT system, making the data (or even the entire system) inaccessible or unusable to authorized users (Centraal Planbureau,, 2016, p. 35; Verizon, 2016, p. 46). Recovery from this kind of infections is by and large not possible, since the data can only be "freed" when the user enters a cryptographic key that only can be obtained via the cybercriminal responsible for the infection (Munnichs et al., 2017, p. 15). While private persons often seem to be rarely inclined to pay a ransom of a few hundred euros (Centraal Planbureau, 2016, p. 35), some sources suggest that businesses generally show a greater willingness to pay to restore their operational integrity and/or protect their reputation (Munnichs et al., 2017, p. 15). According to some sources (e.g., Centraal Planbureau, 2016, p. 38) ransomware-campaigns have become a very lucrative form of cybercrime, not only because of their low cost and the low detection rate, but also because the extortionists can vary the ransom depending on the importance of the data for the business.

In addition to the demand for a ransom, other types of extortion are also prevalent in cyberspace and thus included in the survey. Cybercriminals have been reported (to attempt) to extract "hush money"

[37] Art. 550*ter* Sw.
[38] Art. 4, Convention on Cybercrime, Council of Europe, Budapest, November 23th 2001, *E.T.S.*, nr. 185.
[39] Art. 5, Convention on Cybercrime, Council of Europe, Budapest, November 23th 2001, *E.T.S.*, nr. 185.

from businesses. This can happen after the business in question has become the victim of a data breach and the extortionists subsequently threaten to make the stolen data public (De Cuyper & Weijters, 2016, p. 7; NCSC, 2016, p. 38). Businesses can also receive requests to pay protection money. Businesses that are highly dependent on IT systems for their daily operations can prove attractive targets for this kind of extortion (Van Leiden et al., 2014). Cybercriminals can, for example, conduct a relatively small data breach or a (D)DOS-attack on the business's website, and inform the owner that a more devastating attack can be averted by paying the requested protection money (Munnichs, 2017, p. 20; Van Leiden, De Vries Robbé & Ferwerda, 2007, p. 40).

These forms of cybercrime show great resemblance with the more classic forms of extortion that are performed in the offline world. Therefore, they can be regarded as instances of computer-assisted crime that can be prosecuted by means of the ordinary criminal law.[40] The demand for protection money for example, has been taking place since time immemorial and has long been one of the favorite types of extortion for Italian mafia organizations (Leukfeldt et al., 2009, p. 102).

2.1.5 Internet Fraud

The last type, "internet fraud," is conceptualized in terms of three of the most frequent types of fraud affecting all types of businesses, namely: advance fee fraud, auction fraud, and fraud with internet banking. The first two are covered by the traditional offence of fraud in the Belgian and other national criminal laws.[41] They are, in fact, frauds that can be committed via a computer or another IT system (as well as offline) but do not require the manipulation of data or computer systems (Domenie et al., 2013, p. 17). We have selected these two specific types - advance fee fraud and auction fraud - because they, according to the literature, are among the most frequent types of fraud, and frequently target businesses (e.g., Domenie et al., 2013, pp. 62-64; Leukfeldt et al., 2009 p. 75; Wall, 2007, pp. 90-93). The advance fee fraud typically involves promising the victim a significant share of a large sum of money, in return for a small up-front payment, which the fraudster requires in order to obtain the large sum. If a victim makes the payment, the fraudster either invents a series of further fees for the victim, or simply disappears (Wall, 2007, p. 90). Auction fraud occurs when certain commodities or services are purchased online, prepaid but subsequently never delivered, or appeared of a lower quality than the advertisement postulated (Domenie et al., 2013, p. 44; Van der Hulst & Neve, 2008, p. 56).

Our third type of fraud, internet banking fraud, occurs when cybercriminals ransack other people's or businesses' bank accounts by misappropriating identity information (such as credit cards or stolen banking credentials) of the victims. Such fraud is included in the Council of Europe's definition of computer-related fraud, as it is a special case of fraud committed through "any *input*, alteration, deletion or suppression of computer data" (Art. 8, emphasis added).[42] It can also be prosecuted under

[40] Art. 470 Sw.

[41] Art. 496 Sw.

[42] Instead, we have excluded from our conceptualization of cybercrime the second type of computer-related fraud defined by the Council of Europe's 2001 Convention, that is, fraud committed through "any interference with the functioning of a computer system" (Art. 8), because this is likely to occur much less frequently than the first one. For the same reason, we have also excluded the offence of computer-related forgery, which is also defined by the same convention. This last category also considers "offences related to child pornography" and "offences related to infringements of copyright and related rights." The reasons for excluding the first of these two categories are obvious, as child pornography does not affect businesses. We have excluded copyrights infringements, because businesses are not victim of them through cyber-attacks but rather through users that spread or download their products without authorization. Moreover, there is no consensus both among policy-makers and academics that copyright infringements also constitute a separate form of cybercrime, rather than a consequence of a

Belgian IT law by means of the article referring to computer fraud.[43] In accordance with the Council of Europe's 2001 convention[44], the Belgian legislator created a new offence that criminalized, among other things, the intentional input of computer data[45] into an IT system[46] "with fraudulent or dishonest intent or procuring, without right, an economic benefit for oneself or for another person."

2.2. The Impact, Harms and Costs of Cybercrime

In this project, we carefully bring together the three concepts that, in the literature, have been alternatively used to consider the negative consequences of cybercrime. In particular, we understand the impact of cybercrime as the overall harm of cybercrime, that is, the "sum" of the material harms, or costs, and the non-material harms of cybercrime. We draw on Greenfield and Paoli's (2013) Harm Assessment Framework, to conceptualize harm—and thus impact itself. Specifically, we understand harm as a violation of stakeholders' legitimate interests, thus recognizing that the dominant political morality and the underlying socio-economic conditions play a central part in establishing which interests are regarded as legitimate. Following Greenfield and Paoli (2013), we further assume that businesses—as well as the other "bearers" identified by their taxonomy--experience harms as damages to one or more "interest dimensions" (von Hirsch & Jareborg, 1991, p. 19). In the case of businesses (and of individuals and other private and public-sector entities), these dimensions consist of functional integrity, material support, reputation, and privacy, of which only the harms to material support can be monetized and thus are costs. Following Greenfield and Paoli (2013), who build on von Hirsch and Jareborg (1991) and Sen (1987), we treat these interest dimensions as representing capabilities or pathways for achieving a certain quality of life, referred to as a "standard of living" (von Hirsch & Jareborg, 1991) in the case of individuals, and as "institutional mission" (Greenfield & Paoli, 2013), in the case of public and private entities, including businesses. Below we identify the harms to material support, or costs and subsequently consider the harms to the other interest dimensions.

We speak of harm to material support, or costs, when a corporate entity suffers a material loss, such as damages to its infrastructure or remediation costs. In particular, we distinguish between personnel and other costs. For the personnel costs, we consider the time spent neutralizing a cyber incident, the portion of it that has been outsourced, and the resulting costs. It is worth noting that the internal personnel costs are neither direct nor indirect, as they do not represent an additional cost for the business; rather, they can be considered opportunity cost, because if the business had not been victim of a cyber incident, the personnel could have been employed otherwise. Instead, the portion of the staff time has been outsourced to external consultants or companies to respond to a cybercrime incident generates a direct cost.

As for the other costs, we identify five categories: (1) hard- and software replacement; (2) value of other lost or damaged assets (e.g., data files); (3) money paid to offender; (4) fines and compensation payments, and (5) revenue lost. The first four categories are direct costs, the last one is an opportunity

cybercrime. The European Commission (2013), for example, does not include such infringements in its categorization of cybercrime.

[43] Art. 504*quater* Sw.

[44] Art. 8, a, Convention on Cybercrime, Council of Europe, Budapest, November 23th 2001, *E.T.S.*, nr. 185.

[45] E.g., stolen login data for online banking.

[46] E.g., the banking website usually used by the victim.

cost. We note that not all the five costs are relevant for our five types of cybercrime. The fourth type of cost, money paid to the offender, for example, is only relevant for cyber extortion: it consists of ransom, "protection money", or "hush money", the latter being a sum paid to buy the "silence" of cybercriminals after these have stolen confidential data from a business).

As for the non-material harms, our definitions are as follows.[47] In the case of businesses, we consider functional integrity, as synonym of operational integrity. Given the centrality of this interest dimension, we have split harms to functional integrity in two in our survey, and further distinguish between "the provision of services to (potential) customers" and the business's "internal operational activities."

Damage to a business, NGO, or government's reputation can occur under a variety of circumstances, including those involving an employee, official or representative's participation in a criminal activity. In this respect as well, we follow Greenfield and Paoli, (2013) who argue that such entities experience at least some reputational loss whenever rule- or lawbreaking leaves the impression that they are weak.

Finally, a business, NGO, or government body may also suffer a loss of "privacy." This results from illegal access to, and possible misuse of, the entity's premises, IT systems, or sensitive proprietary information, which might render the entity less able to pursue its institutional interests.

By identifying only the harms to material support as costs, we draw a clear line between those harms that can be monetized from those than cannot. Following Greenfield and Paoli (2013), we regard some harms—such as the harms to individuals' dignity or harms to individuals' and entities' reputation and privacy—as inherently unquantifiable. We recognize that other interest dimensions, such as the functional integrity of a business, can at least in principle and partially be measured through monetary indicators (e.g., stock exchange price), but realize that this data is not available for all businesses nor is it possible to separate the impact on it of each single cybercrime. The clear distinction between costs and other harms gives us, as Greenfield and Paoli (2013, p. 874) argue, "the freedom of employing alternative means of analysis and formally incorporating qualitative insights; we do not, so to speak, leave any credible information on the table." In addition to questions supporting the estimation of the costs, we have envisaged questions in our survey to let respondents to assess the other harms on the basis of a six-point scale of harm severity drawn from Greenfield and Paoli's (2013) framework. In such a way, we give a full conceptualization of impact and avoid the opposed dangers of neglecting the harms that cannot be monetized and of embarking in wacky assumptions to monetize all harms.

Following Greenfield and Paoli (2013), we also set relevant bounds on our assessment. In particular, unlike the cost-of-crime literature (see chapter 1), we exclude the costs incurred by private businesses to protect themselves from crime. There are three reasons for this decision. First, individuals, and in most cases businesses and NGOs, do not assess the threat of each criminal activity separately, making it impossible to identify, let alone estimate, the costs of efforts to prevent each particular activity. Second, prevention costs are not solely a function of the inherent "toxicity" of crime itself, but are also a function of the perceptions of individuals and entities. A business, for example, might incur security expenses, for three reasons: an internal desire to hedge risks, the demand from employees and customers for particular protections, and government regulation mandating certain security measures (Jackson et al., 2007, pp. 34–35). Lastly, prevention costs are often bundled together with general

[47] This conceptualization heavily relies on Greenfield and Paoli (2013).

compliance and technological systems, hence it would be very difficult to disentangle them empirically from the costs of these other activities (Levi & Burrows, 2008, p. 310).

Along the same lines, we exclude law enforcement costs. If we were to include them, the criminal activities that are already most heavily prioritized by law enforcement agencies – as reflected in the agencies' funding and expenditures – would likely appear to be more harmful than other activities that have been less heavily prioritized.

We do, however, consider remediation and replacement costs, such as the costs incurred by a business to respond to a cyber incident, or to repair and substitute assets damaged or stolen by criminals, including increases in insurance premiums that might result from repair or replacement.

3. Methods

In this chapter, we present the project's research design. We start with a brief discussion of the contents of the survey, and continue with the sample construction process and some information about the final sample. Next, we discuss how we constructed the scales from the items questioned. In the final section, we explain the analytical procedures we have followed.

3.1. Survey

We have collected the data via a web-based survey (see appendix A). In the first part of the survey questionnaire, we have asked several general questions to enable the categorization of the businesses on the basis of, inter alia, their size and economic sector. The bulk of the questionnaire was structured on the basis of the cybercrime typology introduced in chapter 1. For each type of cybercrime, the questionnaire followed a similar format and entailed five (sets of) questions, one for each of the five objectives of the study (see introduction).

The first question asked respondents how often their business had been confronted with the selected cybercrime type in the past 12 months. The eight possible answers– ranging from *never* to *hundreds of times a day* – served to direct respondents to the next set of questions. If the answer was *never*, the survey immediately proceeded to the fifth set of questions. In the case of single (*once*) or multiple victimization (*a few times* up to a *hundreds of times a day*), respondents were expected to answer the following sets of questions for this incident. In the case of multiple victimization, we have asked respondents to distinguish in the following sets of questions between the last and the most serious incident for all types, except for illegal access to IT systems. As the latter crime occurs much more frequently than the others (e.g., Clough, 2010: 59; Wall, 2007: 53-54), we have asked respondents to distinguish between the last, and all the previous incidents that occurred during the past 12 months.

The second question entailed a specification of the incident. In the case of cyber extortion, for instance, respondents were invited to specify whether the incident could be best categorized as a demand for money (1) to avert or stop an attack; (2) to unblock systems or data, or (3) to avoid confidential or compromising data from disclosure—items that correspond to the earlier specification of cyber extortion in requests of protection money, ransomware campaigns and requests of hush money.

The third and fourth sets of questions focused on the costs and non-material harms of cybercrime. To investigate the personnel costs, we have first asked the respondents to indicate the total amount of staff time that was needed to respond to/neutralize the incident. Possible answers ranged from *less than an hour* to *more than 2 working months*. By multiplying these figures with the earlier collected data on average personnel cost per hour of the business IT staff, we can thus estimate the personnel costs generated by cybercrime for the businesses that did not outsource such tasks to external consultants. We have also asked respondents to specify which portion of the staff time has been outsourced to external consultants or companies to respond to each incident. For the five other costs we have asked the respondents to estimate the amount of money spent or lost because of the incident. The possible answers here ranged from *less than €1.000,* to *more than €20.000* for internet fraud, and from *nothing*[48] to *more than €200.000,* for the four other types of cybercrime.

[48] We also instructed the respondents to indicate *nothing* if an item was not applicable.

Following Greenfield and Paoli (2013), we conceptualize other harms as harms to the business's functional integrity, reputation and "privacy." We further split functional integrity into two subcategories: internal operational activities, and services to customers. All these harms cannot fully be expressed in monetary terms. It is difficult to put a dollar or euro value on some harms, such as those to privacy. For others, it might be conceptually possible, but the data to do so is insufficient. These problems are also discussed in the cybercrime literature: both Klahr et al. (2016, p. 39) and the NCSC (2016, p. 19) admit that it is very hard to estimate the full economic impact of security breaches. Klahr et al. (2016, pp. 39-40), in particular, note that "it is very uncommon for businesses to have ongoing monitoring of the financial cost of cyber security breaches, with just five per cent of firms saying they do this."

To avoid these problems, we have asked the respondents to assess the severity of the harms to the four interest dimensions on the basis of a six-point scale, including the categories of *no harm, marginal, moderate, serious, grave,* and *catastrophic.* To help the respondents clearly understand the meaning of these terms, we also added following guideline: "In assessing the severity of a harm please consider the ability of your business to fulfil its mission in the mid and long-term (thus six months or longer) as a benchmark:

- A "catastrophic" harm would be a harm that prevents your business from fulfilling its mission for six months or longer;
- At the opposite end, a "marginal" harm is a harm that affects only lightly and/or shortly your business's ability to fulfil its mission;
- Given this long-term perspective, an incident that shuts down all business's services for one day or two would be "serious" or "grave" but not "catastrophic";
- "Not applicable" means that this type of cyber incident cannot (according to you) have an effect upon the item being asked."

The fifth set of questions of the core part of the survey invited the respondents to assess the risk of (another) victimization for each of the five cybercrime types in the next 12 months on a 4-point scale ranging from *very unlikely* to *very likely*.

The final part of survey included some more general questions about cybercrime and had to be filled out by all respondents. Here we first asked the respondents how many times the business had to restart the corporate network from a back-up or restore it from scratch due to cyber incidents in the previous 24 months. We subsequently asked the respondents to assess the harm of cybercrime in general for all businesses within their sector in the previous 12 months. Lastly, we asked the respondents whether the perpetrators of cybercrime incidents endured by their business were insiders or outsiders, and whether they had reported the incidents to the police or other agencies (such as the Cybercrime Emergency Response Team, known as CERT).

3.2. Sample

The target population of the survey consisted of all the businesses based in Belgium. We constructed a sampling frame of 9,249 business representatives based on information provided by the Federation of Enterprises in Belgium (FEB), the largest business consortium in Belgium representing more than 50.000 small, medium and large businesses based in Belgium, and by the sector federations Comeos and

Febelfin. These two federations represent sectors considered particularly vulnerable to cybercrime, i.e., commerce and services as well as banks, stock markets, credit and investment, respectively.

An automatically generated email was sent to all members of the sampling frame, with a unique code to access and resume the survey on LimeSurvey, an online survey software program. The survey was distributed in three languages, Dutch, French and English and ran from June to August 2016—a period during which we sent three reminders (early July, late July, Mid-August).

The number of non-contacts was high: 1,198 business representatives could not be reached, due to undeliverable emails, unavailable mailboxes, or expired e-mail addresses. Of the business representatives who are expected to have received the e-mail, 453 filled out (entirely or partially) the questionnaire, which brings the initial participation rate to 4.9%. This rate is low, but not much lower than the participation rate of the few other studies that explicitly report such rate: in the CSI-study (2011), for example, 6.4% of the contacted businesses participated.[49]

The majority of the businesses that took part in the survey have their headquarters in Flanders (62%). Further, Brussels account for 21% of the sample, and Wallonia 14%. The number of businesses whose headquarters is outside Belgium is considerably lower, amounting to 3.6% of the sample. By comparing these figures with the official data about the location of businesses and persons liable for VAT (FOD Economie, 2016), we note that the percentage of the Flanders-based businesses taking part in the survey corresponds to the percentage of businesses and persons liable for VAT located in Flanders (61%). In our sample, there is instead an overrepresentation of the Brussels-based businesses, as they effectively count only for 11.%, and an underrepresentation of those based in Wallonia, which are in reality about a quarter of the total amount of Belgian businesses and persons liable for VAT (27%).

The businesses taking part in the survey belong to many different economic sectors, but many sectors, and the related sector federations, are only represented once or twice in our sample. The sectors most strongly represented in our sample of respondents are the following: technology (Agoria; 23%), the chemical and life sciences (Essenscia; 10%), and commerce and services (Comeos; 10%). Due to the low number of representatives of many sector federations, we could not make the analysis of the incidence or impact of cybercrime per sector.

As for the size of the businesses, we distinguish between small, medium and large businesses, based on staff headcount, following the standard classification of the European Commission (2003). This defines businesses with less than 50 staff as small, those with a staff between 50 and 249 as medium, and those with more 250 or more staff as large. In our sample, around half of the businesses are small (52%), the rest of the sample being almost equally distributed amongst medium (22.0%), or large (27%) businesses. Comparing these figures with the data of the Belgian Ministry of the Economy (FOD Economie, 2016) on all the businesses and persons liable for VAT, we see that our sample is not representative for the size: according to the Ministry's data, 99% of all the persons and entities liable for VAT are small, 0.6% are medium and 0.2% are large. Specifically, this means that large businesses are underrepresented, and small businesses are overrepresented in our final sample.

[49] Most of the studies about the costs or harms of cybercrime do not provide information on the participation/response rate or the number of contacted units, but only report the number of respondents (e.g. Klahr et al.; 2017; PwC Belgium, 2017; PwC UK, 2015).

3.3. Scale Construction

Although our analysis primarily relies on descriptive statistics, we have combined some items into scales for some specific analyses. We have constructed all scales on the basis of the mean scores on the items, so that they have the same range of answer possibilities as the original items.

With regards to victimization, we have combined the items measuring the incidence of the different cybercrime types in the past 12 months into one scale aimed to measure the incidence of the five types of cybercrime together. The scale ranges from zero to seven, with higher scores representing higher incidences of cybercrime victimization. Reliability analysis, however, showed that the internal consistency of the scale ($\alpha = .479$) was below the general accepted standard of .70 (e.g. DeVellis, 2012; Nunnaly, & Bernstein, 1994). Therefore, we have used this only to describe the percentage of the businesses that had, or had not, been confronted with any of the five cybercrime types.

We have also constructed two scales for the perceived victimization risk in the upcoming 12 months. As a first step, we combined the different items into scales aimed to measure the perceived victimization risk of each of the five types of cybercrime. Each of these scales ranges from zero to three, with higher scores pointing to a higher perceived victimization risk. All of the scales have a good, to very good, internal consistency (ranging from $\alpha = .861$ to $\alpha = .948$). In the second step, we combined the five scales developed in the first step into a single scale intended to measure the perceived victimization risk of cybercrime in general. Ranging from zero to three, this scale, too, has sufficient internal consistency ($\alpha = .834$) to be used in the analyses.

3.4. Data-analysis

We have used SPSS Statistics 24.0 (2016) to analyze the data. First, we have conducted descriptive analyses on all variables, which, as already mentioned, constitute the bulk of our results section.

Second, we have run a series of Analyses of Variance (ANOVA). On the one hand, we have first conducted an ANOVA for business size, business location, and the interaction of these two variables as independent variables, together with the incidence of victimization in the past 12 months as dependent variable for each of the five cybercrime types. On the other hand, we have conducted ANOVAs for the perceived risk of victimization of the five cybercrime types in the next 12 months as dependent variable and size, business location, victimization of the respective type of cybercrime as well as the interactions between these variables as independent variables. For all the analyses, we have used the standard significance level of .05, unless there was a violation of the assumption of homogeneity of variances in an ANOVA. In these cases we tested more conservatively by lowering the significance level to .01.

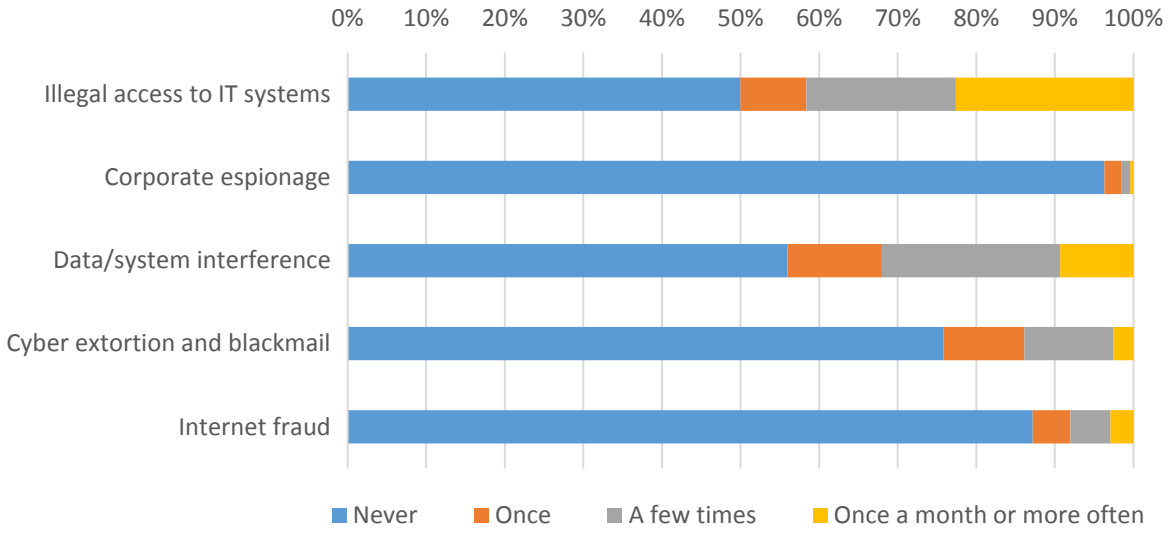
4. Results

In this section we present the results of the empirical study. First, we discuss the extent to which businesses have been confronted with cybercrime in the 12 months preceding the survey, this includes, both the business victimization prevalence for each cybercrime type, and the incidence of each type. Next, we focus on the business representatives' perceptions of the likelihood of their business being attacked in the following 12 months. Third, we estimate the harms to material support, that is, the costs of cybercrime that the businesses have experienced in the 12 months before the survey. Fourth, we discuss the business representatives' assessments of the non-material harm of cybercrime that the businesses have experienced in the same time span.

4.1. Victimization and Incidence of Cybercrime in the Past 12 Months

More than half of the businesses in our sample (67% or 181 businesses) have been victims of cybercrime, at least once in the last 12 months, due to illegal access to IT systems, corporate espionage, data/system interference, cyber extortion, or internet fraud. Specifically, 50% of the businesses (or 155 businesses) have been victim of illegal access to their IT system, 4% (or 10 businesses) of corporate espionage, 44% (or 128 businesses) of data or system interference, 24.1% (or 68 businesses) of cyber extortion, and 13% (or 35 businesses) of internet fraud. Figure 5 provides more insight into the incidence of cybercrime in the 12 months before the survey in our sample.[50]

Figure 5. Incidence of the five types of cybercrime in the sample



Note. Samples sizes varied between 272 (internet fraud) and 310 (illegal access to IT systems). Answer possibilities roughly once a month, roughly once a week, roughly once a day, several times a day and hundreds of times a day were combined into the category once a month or more often to keep the figure clear for the reader.

A majority of the businesses have suffered repeated attacks. The data shows that 83.2% of the 155 victims or report repeated attempts at illegal access to their IT system; 72.7% of the 128 victims experience repeated incidents of data or system interference, and 57.4% of the 68 victims report

[50] Incidences split up by business size and location can be found in appendices B.I.1 and B.I.2.

repeated cyber extortion incidents. Four out of the ten victims experience repeated incidents of corporate espionage and 22 out of the 35 victims experience more than one incident of internet fraud.

We have also examined whether the incidences of the five types of cybercrime differ significantly due to business size and location, and/or the interaction between these two variables. As summarized in table 5, business size results in significant differences in the incidences of illegal access to IT systems, data/system interference, and cyber extortion (F (2, 294) = 7.329, $p < .001$; F (2, 276) = 5.913, $p = .003$; and F (2, 268) = 11.489, $p < .001$).[51] More concretely, small businesses (M = 1.09, SD = 1.81 and M = 0.65, SD = 1.04 respectively) report lesser incidences of illegal access to IT systems, and data/system interference in the past 12 months than large businesses (M = 2.14, SD = 2.06 and M = 1.22, SD = 1.31 respectively).

For illegal access to IT systems – but not for data/system interference (at least not at the predetermined significance level of .01) – the differences between small and medium businesses are also significant: medium businesses (M = 1.79, SD = 2.01) have experienced more incidents of data/system interference in the past 12 months than small businesses (see above for M and SD). Both small (M = 0.17, SD = 0.59), and medium businesses (M = 0.34, SD = 0.68) reported fewer instances of cyber extortion in the past 12 months, than large businesses (M = 0.88, SD = 1.08).

Our analysis also suggests that location does not have a significant effect on the frequency of the five types of cybercrime.

Table 5. Differences in victimization due to size and location

	Illegal access to IT systems	Corporate espionage	Data/system interference	Cyber extortion	Internet fraud
Size	**	ns.	*	**	ns.
Location	ns.	ns.	ns.	ns.	ns.
Size* Location	ns.	ns.	ns.	ns.	ns.

*Note. ns.: not significant, * p < .01, ** p < .001.*

Table 6 summarizes the information we have collected on the techniques used to commit different cybercrime types. The table shows that approximately three quarters of the incidents of illegal incidents to IT systems are committed through the use of hackertools and techniques. In about 60% of the cases, incidents of data/system interference are caused by data traffic (primarily by data sent to the mail server), and in approximately 40% of the cases, by manipulation of data, or systems (primarily PC- and network infrastructure). Almost all incidents of cyber extortion consist of the request for ransom money to unblock the business's IT system. Finally, most of the incidents of internet fraud, consist of fraud with internet banking.

[51] Levene's tests showed that the assumption of equal error variances was respected in the ANOVA's for illegal access to IT systems (F (8, 294) = 1.16, $p = .323$), but not in the ANOVA's for data/system interference (F (8, 276) = 2.14, $p = .032$), cyber extortion (F (8, 268) = 11.89, $p < .001$), corporate espionage (F (8, 263) = 5.79, $p < .001$) and internet fraud (F (8, 259) = 9.45, $p < .001$). As indicated in the methodology section, we used a significance level of .01 instead of .05 in the latter cases.

Table 6. Techniques used to commit cybercrime incidents

Type/technique	Incidents	
	Only/last	Most serious
Percent values		
Illegal access to IT systems		
• Hackertools and techniques	75.3%	71.7%
• Exceeding access privileges by users	7.8%	7.1%
• Exploiting vulnerabilities in security	7.8%	11.0%
• Other	9.1%	10.2%
Data/system interference		
• Data interference		
- Webserver	17.2%	18.8%
- Mailserver	40.2%	37.5%
- Services for online storage of internal documents	4.1%	3.8%
• System interference		
- PC-infrastructure	15.6%	21.3%
- Network infrastructure	18.0%	16.3%
- Peripherals	-	-
- Business website	4.9%	2.5%
Cyber extortion		
• Protection money	10.6%	
• Ransom money	89.4%	
• Hush money	-	
Absolute values		
Corporate espionage		
• Bulk business data	3	
• High value IP	2	
• Tactical corporate information	3	
• Other	1	
Internet fraud		
• Advance fee fraud	8	
• Auction fraud	1	
• Fraud with internet banking	22	

Note. Samples sizes were 154 (only/last) and 127 (all) for illegal access to IT systems, 122 (only/last) and 80 (most serious) for data system interference and 66 for cyber extortion.

4.2. Perceived Risk of Victimization in the Subsequent 12 Months

In addition to their actual experiences as victims, we have let our respondents estimate the risk to their business of being victimized in the coming 12 months for each type of cybercrime. In table 7, we present an overview of the results.[52] We constructed the scales by giving a score of 0 to 3 to the rankings concerning the risk of victimization (thus 0 to *very unlikely* and 3 to *very likely*), and then calculating the mean of the risk assessments of the different subtypes. In a nutshell, most of respondents assess their business's risk of being victimized in the next 12 months, as "very unlikely" or "unlikely," with the exception of illegal access to IT systems. For this last cybercrime type, the most frequent answers chosen by the respondents are "unlikely" and "likely." Especially illegal access to IT systems (via the use

[52] The perceived victimization risks, split up by business size, location and previous victimization, can be found in appendices B.II.1 and B.II.2.

hackertools and techniques) is perceived as likely to occur in the next 12 months. Approximately 60% of the representatives assess their business's probability of experiencing this crime in the next 12 months as "likely" or "very likely."

Table 7. Perceived victimization risk of cybercrime in next 12 months

Type	Perceived risk of victimization				
	Very unlikely (0)	Unlikely (1)	Likely (2)	Very likely (3)	*M* (*SD*)
Illegal access to IT systems					1.41 (0.75)
• Hackertools and – techniques	11.4%	29.2%	33.2%	26.2%	
• Exceeding access privileges by users	21.8%	47.0%	21.8%	9.4%	
• Exploiting vulnerabilities in security	13.7%	44.1%	33.4%	8.7%	
• Other	18.6%	40.7%	30.7%	10.0%	
Corporate espionage					0.83 (0.68)
• Bulk business data	32.8%	49.8%	15.5%	1.9%	
• High value IP	39.6%	44.9%	14.0%	1.5%	
• Tactical corporate information	35.5%	47.9%	15.5%	1.1%	
• Other	34.4%	48.6%	15.8%	1.2%	
Data/system interference					1.13 (0.66)
• Data interference					
- Webserver	20.7%	41.9%	30.0%	7.4%	
- Mailserver	15.6%	41.9%	28.9%	13.7%	
- Services for online storage of internal documents	30.6%	46.3%	17.9%	5.2%	
• System interference					
- PC-infrastructure	18.2%	52.8%	23.0%	5.9%	
- Network infrastructure	22.7%	53.2%	19.3%	4.8%	
- Peripherals	25.8%	56.6%	14.2%	3.4%	
- Business website	20.0%	52.5%	22.6%	4.9%	
Cyber extortion					1.00 (0.73)
• Protection money	28.3%	49.3%	19.9%	2.6%	
• Ransom money	23.0%	42.0%	26.8%	8.2%	
• Hush money	35.3%	47.4%	14.7%	2.6%	
Internet fraud					0.96 (0.77)
• Advance fee fraud	33.2%	40.7%	21.3%	4.7%	
• Auction fraud	37.5%	45.1%	15.0%	2.4%	
• Fraud with internet banking	30.7%	39.8%	21.7%	7.9%	
Total					1.07 (0.57)

Note. Sample sizes varied between 290 and 299 for illegal access to IT systems, 265 and 270 for data/system interference, 269-272 for cyber extortion, 259-265 for corporate espionage and 253-254 for internet fraud. The scales aimed to measure the expected probability of victimization of each type of cybercrime and cybercrime in general had a range from zero to three.

As for the actual victimization, we have also considered whether the perceived risk of victimization differs significantly depending on the business's size and location. For these analyses we also have

considered previous experiences of victimization.[53] Our analysis shows that none of the effects are significant (size: F (2, 244) = 2.94, p = .055); location: F (2, 244) = 2.97, p = .053; victimization: F (1, 244) = 1.78, p = .183).[54]

We also conducted analyses for each type of cybercrime separately. For this analysis, we have used size and location once more as independent variables, but instead of a victimization variable with only two groups (non- victimized businesses and victimized businesses), we have used a three-group victimization variable (non- victimized businesses, businesses victimized once and businesses victimized repeatedly) as the third independent variable, in order to distinguish between single and repeated instances of past victimization.[55] The results are summarized in table 8.

Table 8. Differences in perceived victimization risk in the next 12 months due to business size, location and previous victimization

	Illegal access to IT systems	Corporate espionage	Data/system interference	Cyber extortion	Internet fraud
Main effects					
Size	ns.	ns.	ns.	ns.	ns.
Location	ns.	ns.	ns.	ns.	ns.
Victimization	***	**	**	**	ns.
Interaction effects					
Size*Location	ns.	ns.	ns.	ns.	ns.
Size*Victimization	ns.	ns.	ns.	ns.	ns.
Location* Victimization	ns.	ns.	ns.	ns.	ns.

*Note. ns.: not significant, * p < .05, ** p < .01., *** p < .001.*

We note that neither size, nor location does not significantly account for the differences in the perceived victimization risk for any cybercrime type (illegal access to IT systems: F (2, 267) = 0.20, p = .819 and F (2, 267) = 1.39, p = .251, respectively; corporate espionage: F (2, 246) = 1.80, p = .167 and F (2, 246) = 2.73, p = .067, respectively; data/system interference: F (2, 237) = 1.61, p = .202 and F (2, 237) = 0.83, p = .439, respectively; cyber extortion: F (2, 242) = 0.79, p = .454 and F (2, 242) = 0.61, p = .545, respectively; internet fraud: F (2, 229) = 0.55, p = .576 and F (2, 229) = 0.20, p = .818, respectively).

Previous victimization, however, has a significant effect on the perceived risk of falling victim to an illegal access to IT systems (F (2, 267) = 16.33, p < .001), corporate espionage (F (2, 246) = 4.99, p = .008), data/system interference (F (2, 237) = 6.08, p = .003), and cyber extortion (F (2, 242) = 5.31, p = .006) in the 12 months after the survey. Only for internet fraud, previous victimization does not contribute significantly to the perceived risk of victimization (F (2, 229) = 2.11, p = .123). More specifically, businesses that have been repeat victims of illegal access to IT systems, data/system interference, or cyber extortion in the past 12 months (M = 1.83, SD = 0.64; M = 1.43, SD = 0.73 and M = 1.47, SD = 0.59,

[53] For the sake of completeness, we have also investigated whether there is any interaction effect among size, location and previous victimization.

[54] Only the interaction effect between size and victimization is significant (F (2, 244) = 3.070, p = .048). This means that the business size has a different effect on the business's perceived victimization risk depending on whether the business was victim or not of that specific type of cybercrime type in the 12 months before the survey. As the main effects of size and previous victimization are not significant, the relevance of this interaction effect should not be overrated. None of the other interaction effects (size and location: F (2, 244) = 0.44, p = .783; location and victimization: F (2, 244) = 1.22, p = .296; size, location and victimization: F (4, 244) = 1.034, p = .390) are significant.

[55] In each ANOVA, the assumption of equality of error variances was respected (illegal access to IT systems: F (24, 267) = 1.18, p = .264; data/system interference: F (26, 237) = 0.90, p = .609; cyber extortion: F (25, 242) = 1.00, p = .474; corporate espionage: F (14, 246) = 1.63, p = .072; internet fraud: F (21, 229) = 1.06, p = .391).

respectively) assess their risk of victimization as significantly higher than those that have never been victimized (*M* = 1.09, *SD* = 0.69; *M* = 1.00, *SD* = 0.62 and *M* = 1.39, *SD* = 0.56, respectively). Furthermore, the businesses that have been repeatedly confronted with illegal access to IT systems in the past 12 months (see above for *M* and *SD*) assess the victimization risk of this cybercrime type as significantly higher than those businesses that have been victimized only once (*M* = 1.14, *SD* = 0.66).[56]

4.3. Costs (i.e., Harms to Material Support)

As concerns costs and harms, we only analyze the data concerning illegal access to IT systems, data/system interference and cyber extortion; for illegal access to IT systems, we also consider the data on the costs and harms of all incidents recorded in the past 12 months, and for data/system interference, that on the most serious incident.[57] As the number of businesses admitting victimization of either corporate espionage (n =9) or internet fraud (n =31) were below 40, the number we used as cut-off point for reporting percent values, we only present the absolute figures in the tables for these two types.

As noted earlier, we have operationalized the costs (that is, harms to material support), through:

- the internal and outsourced staff time and the related costs invested in neutralizing cyber incidents
- the business's assessment of four direct costs—(1) hardware and software replacement, (2) value of other lost or damaged assets (e.g., data files), (3) the money paid to offender and (4) fines and compensation payments—as well as the opportunity cost of potential revenue lost.[58]

Table 9 summarizes the responses about the internal staff time invested in neutralizing incidents of four cybercrime types, excluding internet fraud. We have excluded the latter cybercrime because we have assumed that no IT staff is needed to deal with it. As table 9 indicates, most respondents reported that they resolved the only or last incident in less than one business day (illegal access to IT systems: 82%; data/system interference: 80%; cyber extortion: 68%). However, between 18% and 32% of these incidents required more than one business day to be neutralized (illegal access to IT systems: 18%; data/system interference: 20%; cyber extortion: 32%) a percentage that grows up to more than 49.2% for all incidents of illegal access recorded in the last 12 months.

[56] We do not interpret the significant result for corporate espionage, distinguishing between single and repeat victimization, because of the small group size of single and repeat victims of this cybercrime type.
[57] This distinction is not possible for cyber extortion, because the number of repeat victims was below the cut-off value of 40.
[58] As earlier noted, not all the five costs are relevant for our five cybercrime types.

Table 9. Staff time invested in neutralizing the cyber incidents suffered

Type		Staff time invested				
		< 1 hour	1 hour – < Half a day	Half a day – < 1 day	1 day – < 1 week	1 week or more
Percent values						
• Illegal access to IT systems	Only/last	32.0%	28.1%	21.6%	14.4%	3.9%
	All	16.7%	15.1%	19.0%	29.4%	19.8%
• Data/system interference	Only/last	20.3%	34.1%	25.2%	18.7%	1.6%
	Most serious	15.2%	27.8%	29.1%	22.8%	5.1%
• Cyber extortion	Only/last	12.1%	30.3%	25.8%	24.2%	7.6%
Absolute values						
• Corporate espionage	Only/last	-	2	3	3	-

Note: Sample sizes are 153 (only/last) and 126 (all) for illegal access, 123 (only/last) and 79 (most serious) for data/system interference, and 66 for cyber extortion. [59]

In table 10 we consider which portion of the staff time invested in neutralizing the cyber incidents has been outsourced to external businesses or consultants. Outsourcing occurs in less than half of all incidents, but the neutralization of data/system interference is outsourced more frequently than that of other cybercrime types, with no substantial differences between the only/last and most serious incidents. In fact, the only/last incidents of illegal access to IT systems, cyber extortion have been dealt with in more than half of the cases without external business or consultants, whereas this percentage decreases to 42% in the case of incidents of data/system interference. The latter type of cybercrime is likely to be considered the most complicated to deal with, as its neutralization is also most frequently fully outsourced: 27% of the only/last incidents of data/system interference are fully outsourced, whereas this percentage decreases to 15% in the case of illegal access to IT systems and 6% for cyber extortion.

Table 10. Staff time invested in neutralizing the cyber incidents suffered which was outsourced to external businesses or consultants

Type		Outsourced staff time				
		None	< Half	Half	Most	All
Percent values						
• Illegal access to IT systems	Only/last	56.9%	11.8%	7.2%	9.2%	15.0%
	All	49.2%	14.8%	10.7%	10.7%	14.8%
• Data/system interference	Only/last	42.4%	10.2%	8.5%	11.9%	27.1%
	Most serious	41.8%	12.7%	11.4%	12.7%	21.5%
• Cyber extortion	Only/last	68.2%	7.6%	6.1%	12.1%	6.1%
Absolute values						
• Corporate espionage	Only/last	5	2	-	-	1

Note. Samples sizes are 153 (only/last) and 122 (all) for illegal access, 118 (only/last) and 79 (most serious) for data/system interference, and 66 for cyber extortion.

Table 11 presents the estimates of the costs of the internal staff time invested in the neutralization of cybercrime for the businesses that do not outsource such tasks. Here we multiply the internal staff time

[59] We have not asked this question for internet fraud, because we have assumed that no IT staff is needed to deal with it.

figures with the data about the average personnel cost per hour of the business IT staff, which we have collected in the initial part of the survey. Respectively 54% and 51.2% of the businesses reporting about the only/last incidents of data/system interference and cyber extortion indicate that the internal staff costs were not higher than €229; in the case of the only or last incident of illegal access to IT systems this percent exceeds 70%. Even for the only/last incident, though, considerable minorities report costs higher than €458 for the neutralization of the incidents: 10.5% for illegal access, 16% for data/system interference and 22% for cyber extortion. This percentage increases to 43.4% for all incidents of illegal access to IT systems.

Table 11. Internal staff costs of the cyber incidents suffered

Type		Costs					
		€1 - €60	€60 - €229	€229 - €458	€458 - €2,290	€2,290 - €4,581	€4,581 - €18,324
Percent values							
• Illegal access to IT systems	Only/last	44.2%	29.1%	16.3%	9.3%	-	1.2%
	All	28.3%	11.7%	16.7%	26.7%	11.7%	5.0%
• Data/system interference	Only/last	20.0%	34.0%	30.0%	14.0%	2.0%	-
• Cyber extortion	Only/last	15.6%	35.6%	26.7%	15.6%	6.7%	-
Absolute values							
• Corporate espionage	Only/last	1	1	3	-	-	-

Note. Samples sizes are 86 (only/last) and 60 (all) for illegal access, 50 for data/system interference, and 45 for cyber extortion.

Tables 12-15 present the data collected on other costs (or harms to material support) that are relevant for each cybercrime type. As table 12 shows, more than half of the businesses have had no costs for replacing hardware or software after suffering illegal access to their IT systems (56%), data/system interference (58%) or cyber extortion (67%). Only between 1.5% and 4% of the businesses report replacement costs of €10,000 or more due to the only/last incident of illegal access to their IT systems, data/system interference or cyber extortion – and the order of magnitude remains similar for all cases of illegal access to IT systems and for the most serious incident of data/system interference.

Table 12. Costs of hard- and software replacement for the cyber incidents suffered

Type		Costs					
		Nothing	€ 1 - €9,999	€10,000 – €49,999	€50,000 - €99,999	€100,000 or more	Don't know
Percent values							
• Illegal access to IT systems	Only/last	55.6%	35.8%	2.0%	-	2.0%	4.6%
	All	50.4%	39.0%	6.5%	0.8%	0.8%	2.4%
• Data/system interference	Only/last	57.5%	33.7%	2.5%	-	-	3.3%
	Most serious	53.1%	40.7%	2.5%	-	1.2%	2.5%
• Cyber extortion	Only/last	66.7%	28.8%	1.5%	-	-	3.0%
Absolute values							
• Corporate espionage	Only/last	4	3	-	-	-	2

Note. Samples sizes are 151 (only/last) and 123 (all) for illegal access, 120 (only/last) and 81 (most serious) for data/system interference, and 66 for cyber extortion.

We have assumed that the second cost, that is, the value of other lost or damaged assets, is only relevant for corporate espionage, data/system interference and cyber extortion. Table 13 illustrates that more than half of the businesses victim of cyber extortion report no lost or damaged assets. For data/system interference this percentage increases to over 60% for the most serious incident and over 70% for the only/last incident. Only 9% of the businesses suffering cyber extortion report costs of €10,000 or more; for data/system interference, the percentage is in all cases lower than 3%.

Table 13. Value of other assets lost or damaged as a result of the cyber incidents suffered

Type		Costs					
		Nothing	€ 1 - €9,999	€10,000 – €49,999	€50,000 - €99,999	€100,000 or more	Don't know
Percent values							
• Data/system interference	Only/last	71.7%	15.8%	0.8%	-	0.8%	10.8%
	Most serious	64.2%	17.3%	1.2%	-	1.2%	16.0%
• Cyber extortion	Only/last	50.0%	25.8%	1.5%	3.0%	4.5%	15.2%
Absolute values							
• Corporate espionage	Only/last	1	3	-	1	1	3

Note. Samples sizes are 120 (only/last) and 81 (most serious) for data/system interference, and 66 for cyber extortion.

In the case of cyber extortion we have asked whether businesses have paid ransom, "protection", or "hush" money to the offender. Only 6% of the businesses suffering cyber extortion did so; in any case the ransom paid remained below €10.000.

As shown in table 14, for cyber extortion as well as for illegal access to IT systems (only/last and all), and the only/last incidents of data/system interference, more than 90% of the businesses report paying no fines or compensation to injured parties. Only for the most serious incidents of data/system interference, the percentage slightly decreases to 86%.

Table 14. Fines and compensation payments as a result of the cyber incidents suffered

Type		Costs					
		Nothing	€ 1 - €9,999	€10,000 – €49,999	€50,000 - €99,999	€100,000 or more	Don't know
Percent values							
• Illegal access to IT systems	Only/last	90.7%	4.0%	-	-	-	5.3%
	All	91.9%	3.3%	-	-	-	4.9%
• Data/system interference	Only/last	93.3%	3.4%	0.8%	-	-	2.5%
	Most serious	86.4%	7.4%	1.2%	-	-	4.9%
• Cyber extortion	Only/last	90.9%	6.1%	-	-	-	3.0%
Absolute values							
• Corporate espionage	Only/last	5	2	-	-	-	2

Note. Samples sizes are 151 (only/last) and 123 (all) for illegal access, 119 (only/last) and 81 (most serious) for data/system interference, and 66 for cyber extortion.

Finally, a large majority of the businesses also indicate that they have not lost any revenue because of cyber incidents, even if there are considerable differences from one cybercrime type to the other (see

table 15). The percentage experiencing no loss is—unsurprisingly— the highest for illegal access to IT systems (only/last: 77%; all: 72%), followed by cyber extortion (only/last: 73%), and data/system interference (only/last: 62% and most serious: 60%). However, between 11% and 24% of the businesses estimate losing between €1 and €9,999 because of one of these three cybercrime types. Much smaller percentages of businesses confronted with illegal access to their IT system (only/last: 3.3%; all: 3.2%) and data/system interference (only/last: 5.8%; most serious: 6.3%) admit suffering losses of €10,000 or more.

Table 15. Lost business as a result of the cyber incidents suffered

Type		Costs					
		Nothing	€ 1 - €9,999	€10,000 – €49,999	€50,000 - €99,999	€100,000 or more	Don't know
Percent values							
• Illegal access to IT systems	Only/last	76.8%	11.3%	2.6%	-	0.7%	8.6%
	All	72.4%	14.6%	0.8%	1.6%	0.8%	9.8%
• Data/system interference	Only/last	61.7%	20.8%	3.3%	1.7%	0.8%	11.7%
	Most serious	60.0%	22.1%	1.3%	2.5%	2.5%	15.0%
• Cyber extortion	Only/last	72.7%	24.2%	-	-	-	3.0%
Absolute values							
• Corporate espionage	Only/last	2	3	1	-	1	2

Note. Samples sizes are 151 (only/last) and 123 (all) for illegal access, 120 (only/last) and 80 (most serious) for data/system interference, and 66 for cyber extortion.

In the case of internet fraud, 22 of the 33 businesses victimized report revenue losses lower than €1,000 due to the only/last incident, four report losses between €1,000 and €10,000 and three report losses higher than €10,000. Two businesses do not provide an amount.

4.4. Harms to Other Interest Dimensions

In table 16 we summarize the businesses' assessment of the severity of the harms caused by cybercrime to three interest dimensions, functional integrity (split up into service to customers and internal operational integrity), reputation, and privacy. For this assessment, respondents could choose among six ratings: *none*, *marginal*, *moderate*, *serious*, *grave* and *catastrophic*. In our comments on this data, we combine the ranking of marginal and moderate, as well as serious and grave, to better illustrate the key points.

For the three cybercrime types for which we have substantial data (i.e., illegal access, data/system interference 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. Between 41% and 66% of the businesses victimized, for example, report no harm to these last three dimensions. Instead, the percent of no harm generally decreases to about 20% in the case of internal operational activities (all cases of illegal access: 22%; only/last incident of data/system interference: 18.3%; and only/last incident of cyber extortion: 19.7%).

Even for the services to customers, reputation, and privacy, between 35% and 50% of the victimized businesses report marginal or moderate harm to these three interest dimensions, with slightly higher

percentages for all the incidents of illegal access and the most serious cases of data/system interference. Five to ten percent of victimized businesses have experienced serious or grave harm to one or more of these three interest dimensions, a percentage that goes up to 13.4% for service to customers after the most serious incident of data/system interference. Moreover, in the case of cyber extortion, small percentages of the businesses victimized suffer catastrophic harms to the services to customers (3.1%), reputation (1.6%), and privacy (3.3%).

Respondents consistently rank the harms to internal operational activities higher. Only for the only or last case of illegal access, one third of the respondents report no harm, otherwise the percent of no harm is as low as 20%. Between 50% and 63% of the victimized business have experienced marginal or moderate harm to their internal operational activities, and between 14% and 20% report serious or grave harm. About 1% of the victimized business even admit catastrophic harm to their internal operational activities because of illegal access or data/system interference. For cyber extortion, the percentages are higher. For the only or last incident of this cybercrime type, 17% of the businesses describe the harm suffered as serious or grave, and 5% admit having suffered catastrophic harm.

In the case of corporate espionage and internet fraud, there is no interest dimension that appears to be more affected than the other ones (but the data should to be interpreted with great caution) due to the low numbers. The businesses that were victim of corporate espionage (*n* = 7 or 8), provide the following harm assessments of the only or last incident:

- Services to customers: one reports no harm, five report marginal or moderate harm, one reports serious harm and one catastrophic harm to this interest dimension;
- Internal operational activities: one reports no harm, five report marginal or moderate harm, one reports grave harm and one catastrophic harm to this interest dimension;
- Reputation: one reports no harm, five report marginal or moderate harm, one reports serious harm and one catastrophic harm to this interest dimension;
- Privacy: two report no harm, three report marginal or moderate harm, one reports serious harm and one catastrophic harm to this interest dimension.

The businesses that fell victim to internet fraud (*n* = 27 or 28) assess the harm of the only/last incident as follows:

- Services to customers: 16 report no harm, seven marginal or moderate harm and five serious or grave harm;
- Internal operational activities: 13 report no harm, 12 marginal or moderate harm and four serious or grave harm to this interest dimension;
- Reputation: 14 report no harm, ten marginal or moderate harm and four serious or grave harm to this interest dimension;
- Privacy: 15 report no harm, nine marginal or moderate harm and three serious or grave harm to this interest dimension.

None of the victims of internet fraud assess the harm to one of the four interest dimensions as catastrophic.

Table 16. Harms to other interest dimensions resulting from the five cybercrime types and the businesses' assessment of the severity of the harms

Type		Harm					
		None	Marginal	Moderate	Serious	Grave	Catastrophic
Percent values							
Illegal access							
• Services to customers	Only/last	51.9%	24.8%	15.0%	5.3%	3.0%	-
	All	41.0%	30.5%	21.0%	4.8%	2.9%	-
• Int. operational activities	Only/last	33.3%	29.8%	22.7%	7.1%	6.4%	0.7%
	All	22.0%	33.0%	29.4%	11.0%	3.7%	0.9%
• Reputation	Only/last	48.9%	31.9%	10.4%	5.9%	3.0%	-
	All	49.5%	28.6%	14.3%	4.8%	2.9%	-
• Privacy	Only/last	48.9%	25.2%	16.3%	3.7%	5.9%	-
	All	47.6%	31.1%	17.5%	1.0%	2.9%	-
Data/system interference							
• Services to customers	Only/last	44.6%	23.2%	22.3%	8.0%	1.8%	-
	Most serious	33.3%	32.0%	21.3%	10.7%	2.7%	-
• Int. operational activities	Only/last	18.3%	32.5%	30.8%	12.5%	5.0%	0.8%
	Most serious	20.3%	34.2%	24.1%	12.7%	7.6%	1.3%
• Reputation	Only/last	45.1%	32.7%	14.2%	5.3%	2.7%	-
	Most serious	51.9%	23.4%	15.6%	6.5%	2.6%	-
• Privacy	Only/last	57.7%	24.3%	9.9%	3.6%	4.5%	-
	Most serious	65.8%	22.4%	2.6%	2.6%	6.6%	-
Cyber extortion							
• Services to customers	Only/last	46.2%	30.8%	12.3%	3.1%	4.6%	3.1%
• Int. operational activities		19.7%	42.4%	16.7%	6.1%	10.6%	4.5%
• Reputation		57.8%	26.6%	7.8%	4.7%	1.6%	1.6%
• Privacy		55.7%	26.2%	9.8%	3.3%	1.6%	3.3%
Absolute values							
Cyber espionage							
• Services to customers	Only/last	1	3	2	1	-	1
• Int. operational activities		1	3	2	-	1	1
• Reputation		1	3	2	1	-	1
• Privacy		2	2	1	1	-	1
Internet fraud							
• Services to customers	Only/last	16	6	1	3	2	-
• Int. operational activities		13	8	4	2	1	-
• Reputation		14	8	2	3	1	-
• Privacy		15	6	3	2	1	-

Note. Samples sizes vary between 133 and 141 (only/last) and 103 and 109 (all) for illegal access, 112 and 120 (only/last) and 75 and 79 (most serious) for data/system interference, and 61 and 66 for cyber extortion.

4.5. The expected impact of cybercrime

We have also asked the businesses to assess the severity of the harms they expect for their whole sector as a result of cybercrime in general. In particular, we have asked businesses to rate the severity of harms arising from cybercrime, and affecting all the interest dimensions of Greenfield and Paoli's conceptualization, thus including also harms to material support, which we have conceptualized for the past in terms of costs. As shown in table 17, approximately 40% of the businesses assess the harm of cybercrime to the material support and finances of businesses of their sector, as serious or higher (serious or grave: 38%; catastrophic: 2%). For the other interest dimensions, the percentage of businesses that assess the harm of cybercrime as serious or higher, is close to 50% (services to (potential) customers: 42% for serious or grave harm, and 5% for catastrophic harm), or even higher than 50% (internal operational activities: 53% for serious or grave harm and 2% for catastrophic harm; reputation with customers and business partners: 49% for serious or grave harm and 5% for catastrophic harm; ability to maintain private data: 51% for serious or grave harm and 8% for catastrophic harm; reputation of whole sector: 47% for serious or grave harm and 4% for catastrophic harm).

Table 17. The expected harms of cybercrime and the businesses' assessment of the severity of such harms for their own sector

Interest dimension	Harm				
	Marginal	Moderate	Serious	Grave	Catastrophic
Finances	20.7%	39.1%	21.9%	16.4%	2.0%
Services to (potential) customers	15.6%	37.5%	24.2%	18.0%	4.7%
Internal operational activities	10.9%	34.6%	29.2%	23.3%	1.9%
Reputation	12.5%	33.2%	28.9%	20.3%	5.1%
Privacy	10.6%	30.7%	28.3%	22.4%	7.9%

Note. Sample sizes varied between 254 (privacy) and 257 (internal operational activities).

Conclusions

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. Illegal access to IT systems;
B. Corporate espionage;
C. Data and system interference:
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.[60] "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," draws from the offence of computer-related fraud defined by the Convention (Council of Europe, 2001: 6; art. 8) as well as two other more traditional types of fraud that frequently target businesses online.

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[61]; (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 business's functional integrity—which we split into internal operational activities and services to customers—reputation and "privacy." Harms to privacy might be caused, for example, by illegal 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.*

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

[61] 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.

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 perceived victimization risk depend on the businesses' size, location, and/or previous victimization experiences (in the latter case).

In the spring and summer of 2016, we sent automatically generated emails, with codes to access and resume the survey, to 9,249 representatives of Belgian businesses. In total, 453 business representatives completed the survey. The questionnaires of 310 of them could be retained for statistical analyses.

Victimization and incidence: The survey results indicate that a large number of Businesses are victims of cybercrime. In total, two thirds (66.5%) 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 illegal access to IT systems (50%), and data/system interference (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. With regards to illegal access to IT systems 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 illegal 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 illegal access to IT systems, data/system interference, 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:[62] The large majority of the last or only incidents are resolved in less than one day (illegal access to IT systems: 82%; data/system interference: 80%; cyber extortion: 68%). However, between 20% and 30% of the incidents require more than one day to be neutralized - a percentage that grows up to more than 49% for all incidents of illegal access recorded in the last 12 months. Most of the reported incidents

[62] 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 illegal access to IT systems, data/system interference, and cyber extortion, for which we have more reliable data.

are addressed by the internal staff. Outsourcing occurs in less than half of all incidents, but the neutralization data/system interference incidents is outsourced more frequently than that of other types of cybercrime; there are no substantial differences between the only or last and the most serious incidents.

The internal staff costs for neutralizing cybercrime incidents tend to be rather low: for the three crime types, more than half – in the case of illegal access to IT systems even more than 70% – of the victimized businesses report cost not higher than €229 due to the only or last incident. However, considerable minorities (that is, 10.5% of the businesses victim of illegal access, 16% of those victim and data/system interference and 22% of those victim of cyber extortion) report costs higher than €458 for the neutralization of the only or last incident – a percentage which increased up to more than 40% for all the incidents of illegal access to IT systems.

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 illegal access to their IT system, data/system interference, or cyber extortion. However, between 1.5% and 4% of the businesses report replacement costs of €10,000 or more due to the only or last incident of illegal access to their IT system, data/system interference, or cyber extortion.

Half of the businesses that are victims of cyber extortion report no lost or damaged assets. For data/system interference, this percentage goes up to 60% for the most serious incident, and 70% for last or only incident.[63] Only 9% of the businesses suffering cyber extortion report costs of €10,000 or more; for data/system interference, the percentage is in all cases lower than 3%.

Among the victims of cyber extortion, 94% indicates that they have paid no money to offenders. For the latter crime as well as for illegal access (only/last and all), and the only/last incidents of data/system interference, more than 90% of the businesses report paying no fines or compensation to injured parties. Only for the most serious incidents of data/system interference, the percentage slightly decreases to 86%.

Finally, a large majority of the businesses also indicate that they have not lost any revenue because of cyber incidents, even if there are considerable differences from one cybercrime type to the other. The percentage experiencing no loss is the highest for illegal access to IT systems (only/last: 77%; all: 72%), followed by cyber extortion (only/last: 73%), and data/system interference (only/last: 62% and most serious: 60%). However, between 11% and 24% of the businesses estimate losing between €1 and €9,999 because of one of these three cybercrime types. Much smaller percentages of businesses confronted with illegal access to IT systems and data/system interference admit suffering losses of €10,000 or more.

Non-material harm: The businesses suffering illegal access to their IT system, data/system interference and cyber extortion consistently report that internal operational activities are more seriously affected than the other three dimensions namely, services to customers, reputation and privacy. Between 41% and 66% of the businesses victimized, for example, report no harm to these last three dimensions.

[63] We have investigated this cost only for data/system interference, cyber extortion and corporate espionage.

Instead, the percent of no harm generally decreases to about 20% in the case of internal operational activities.

Even for the services to customers, reputation, and privacy, between 35% and 50% of the victimized businesses report marginal or moderate harm to these three interest dimensions, with slightly higher percentages for all the incidents of illegal access and the most serious cases of data/system interference. Five to ten percent of victimized businesses have experienced serious or grave harm to one or more of these three interest dimensions, a percentage that goes up to 13.4% for service to customers after the most serious incident of data/system interference. Moreover, in the case of cyber extortion, small percentages of the businesses victimized (< 5%) suffer catastrophic harms to the services to customers, reputation, and privacy.

Respondents consistently rank the harms to internal operational activities higher. With the exception of the only or last case of illegal access to IT systems (around 33%), the percent of businesses suffering no harm to internal operational activities is only 20% . Between 50% and 63% of the victimized businesses have experienced marginal or moderate harm to their internal operational activities, and between 14% and 20% report serious or grave harm. About 1% of the victimized business even admit catastrophic harm to their internal operational activities because of illegal access or data/system interference.[64] For cyber extortion, the percentages are higher. For the last/only incident of this cybercrime type, 17% of the businesses describe the harm suffered as serious or grave, and 5% admit having 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.

Our findings are more conservative than those reported by private security and consultancy companies, but appear to be higher than those reported by other academic studies, even if they are no directly comparable (e.g., Anderson et al., 2013; Klahr et al., 2017). We can only speculate about the source of the differences, given the different period and national context of the studies and the different methodologies adopted. The difference, in particular, might be due to the clear distinction between costs and harms in our typology; this might have encouraged businesses to report harms that previously remained hidden, because the businesses were forced to provide a monetary estimation of such harm.

[64] In all these cases, there are no major differences between last/only and all/most serious incidents.

It is important to keep in mind that our empirical test suffers from considerable limitations, as with most other studies on cybercrime[65] and, more generally, many studies relying on individuals' of businesses' accounts of their victimization. The most important limitation is that we did not use a probability sample, but a convenience sample, which has turned out to be unrepresentative of the distribution of Belgian businesses based on their size and location. Therefore, our results cannot be generalized to all Belgian businesses. Second, the non-participation rate in our study has been very high (approximately 95%). This may be due to several reasons such as the high sensitivity of the topic, limited return of the survey to participants, survey length, etc. We have no information about the characteristics of the non-respondents, but we cannot exclude the possibility that the non-response was selective, which would increase the magnitude of the bias in our estimates. Given the nature of the crime, our results might also underestimate the actual rates of victimization, and/or the actual costs and harms of the cyber incidents reported. The businesses, or our respondents, might not have been (fully) aware of some cyber incidents or their impact or might not have been willing to admit either of them.

We are also aware that, on the basis of past events, it is hard to make predictions of the expected incidence and harms of a crime that, according to most observers, is still expected to grow very rapidly, if not exponentially, in the years to come (e.g., ENISA, 2015). Given the growing connectivity of society, the upcoming "Internet of Things," and the increasing dependence of most businesses on digital technology, these are likely to suffer cybercrime with increasing frequency and severity. The predictive power of the assessment can be improved if it is repeated at regular intervals and thus gains the trust of a greater number of respondents.

Our approach produces less "sexy" results than other studies delivering impressively high and precise figures of the costs of cybercrime (e.g., Detica, 2011; CSIS, 2014). As we have seen, though, many, if not all, previous studies delivering exact figures suffer from serious deficiencies and ultimately produce figures that run the risk of being meaningless (Florêncio & Herley, 2011; Wall, 2008). As John Maynard Keynes, possibly the most influential economist of the 20th century, put it, it is better to "be vaguely right, rather than precisely wrong." In a world in which private security companies and self-proclaimed experts often try to outbid each other, with ever more alarming figures and projections, our study endeavors to be the first, independent, rigorous assessment of the intrinsic costs and harms suffered by Belgium-based businesses because of cybercrime. Furthermore, our assessment is supported by a conceptual framework and research design that can be replicated in future studies.

[65] The only possible exception is Klahr et al. (2017), who use a large random probability sample.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265-300). New York, NY: Springer.

Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime economic costs: No measure, no solution. In B. Akhgar & B. Brewster (Eds.), *Combatting cybercrime and cyberterrorism: Challenges, trends and priorities* (pp. 135-156). Basel, Switzerland: Springer.

Bernaards, F., Monsma, E., & Zinn, P. (2012). *High tech crime: Criminaliteitsbeeldanalyse 2012 [High tech crime: Criminality analysis 2012].* Woerden, The Netherlands: Korps Landelijke Politiediensten.

Boie, J. (2015, November 4). Hackerangriff war was? [Was it an hacker attack?]. *Süddeutsche Zeitung*. Retrieved from http://www.sueddeutsche.de/politik/hackerangriff-war-was-1.2722482?reduced=true

Brand, S., & Price, R. (2000). *The economic and social costs of crime.* London, UK: Home Office.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *The Economic impact of cyber-attacks.* Retrieved from https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf.

Caulkins, J.P., Reuter, P., & Coulson, C. (2011). Basing drug scheduling decisions on scientific ranking of harmfulness: False promise from false premises, *Addiction, 106,* 1886–1890. doi: 10.1111/j.1360-0443.2011.03461.

Centraal Planbureau (2016). *Risicorapportage cyberveiligheid economie [Risk reporting cyber security economy].* Retrieved from www.cpb.nl.

Centre for the Protection of National Infrastructure [CPNI] (2014). *Cyber-attacks: Effects on UK Companies.* Retrieved from http://www.oxfordeconomics.com/my-oxford/projects/276032.

Center for Strategic and International Studies (2014). *Estimating the global cost of cybercrime: Economic impact of cybercrime II.* Retrieved from https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Clarkson, C., Cretney, A., Davis, G., & Shepherd, J. P. (1994). Assaults: The relationship between seriousness, criminalisation and punishment. *Criminal Law Review, 4,* 4-20.

Clough, J. (2015). *Principles of cybercrime (2nd ed.).* Cambridge, UK: Cambridge University Press.

Cohen, M. A. (1988). Pain, suffering and jury awards: A study of the cost of crime to victims. *Law and Society Review, 22,* 537-555. doi: 10.2307/3053629

Cohen, M. A. (2005). *The costs of crime and justice.* London, UK: Routledge.

Cohen, M.A. , & Piquero, A. R. (2009). New evidence on the monetary value of saving a high risk youth. *Journal of Quantitative Criminology, 25,* 25-49. doi: 10.1007/s10940-008-9057-3

Cohen, M. A., Rust, R. T., Stehen, S., & Tidd, S. (2004). Willingness-to-pay for crime control programs. *Criminology, 42,* 89-110. doi: 10.1111/j.1745-9125.2004.tb00514.x

Computer Security Institute [CSI]. (2011). *15th Annual 2010/2011 Computer Crime and Security Survey.* Retrieved from https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

Corkery, M. (2016, April 30). Hackers' $81 million sneak attack on world bank. *The New York Times.* Retrieved from https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html?_r=0

Czabański, J. (2008). *Estimates of cost of crime: History, methodologies and implications.* Berlin, Germany: Springer.

De Cuyper, R. H., & Weijters, G. (2016). *Cybercrime in cijfers: Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices [Cybercrime in numbers: Exploring the possibilities of including cybercrime in the National Safety Indices].* Retrieved from www.wodc.nl

Deloitte (2016). *Cyber value at risk in the Netherlands.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-cyber-value-at-risk.pdf

Detica (2011). *The cost of cybercrime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office.* Guilford, UK: Detica.

DeVellis, R. F. (2012). *Scale development: Theory and applications (3rd ed.)*. Thousand Oaks, CA: Sage.

Diamond, B., & Bachmann, M. (2015). Out of the beta phase: Obstacles, challenges, and promising paths in the study of cyber criminology. *International Journal of Cyber Criminology, 9*, 24-34. doi: 10.5281/zenodo.22196

Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J. A., Jansen, J., & Stol, W. Ph. (2013). *Victimisation in a Digitised Society – A Survey Among Members of the Public Concerning E-fraud, Hacking and Other High-Volume Crimes.* The Hague: Eleven International Publishing.

Dorn, N., & van de Bunt, H. (2010). *Bad thoughts: Towards an organised crime harm assessment and prioritisation system (OCHAPS).* Rotterdam, The Netherlands: Erasmus University.

Dubourg, R., & Prichard, S. (2007). The impact of organised crime in the UK: Revenues and economic and social costs. In Home Office (Ed.), *Organised crime: Revenues, economic and social costs, and criminal assets available for seizure* (pp. 1-53). London, UK: Home Office.

Dugan, L. (1999). The effect of criminal victimization on a household's moving decision. *Criminology, 37,* 903-928. doi: j.1745-9125.1999.tb00509.x

Dutton, R. E., & Hemphill, K. J. (1992). Patterns of socially desirable responding among perpetrators and victims of wife assault. *Violence and Victims, 7,* 29-39.

Espiner, T. (2011, February 18). Cybercrime cost estimate is 'sales exercise', say experts. *ZD Net.* Retrieved from http://www.zdnet.com/article/cybercrime-cost-estimate-is-sales-exercise-say-experts/

European Commission (2003). Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. *Official Journal of the European Union,* 124, 36-41.

European Commission (2007). *Towards a general policy on the fight against cybercrime.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14560

European Commission (2013,). *Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity strategy of the European Union: An open, safe and secure cyberspace.* Retrieved from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Law Enforcement Agency [Europol] (2013). *Europol SOCTA 2013: EU serious and organized crime threat assessment.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013

European Law Enforcement Agency [Europol] (2016). *Internet Organised Crime Threat Assessment 2016.* Retrieved from https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

European Law Enforcement Agency [Europol] (2017). *SOCTA 2017: European Union serious and organized crime threat assessment: Crime in the age of technology.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017

European Union Agency for Network and Information Security [ENISA] (2016a). *ENISA threat landscape 2015.* Retrieved from www.enisa.europe.eu.

European Union Agency for Network and Information Security [ENISA] (2016b). *The cost of incidents affecting CIIs.* Retrieved from https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/at_download/fullReport

Fattah, E. A. (2010). The evolution of a young and promising discipline: Sixty years of victimology, a retrospective and prospective look. In S. G. Shohan, P. Knepper, & M. Kett (Eds.), *International handbook of victimology* (pp. 43-94). Boca Raton, FL: CRC Press.

Federale Regering (2016). *Kadernota integrale veiligheid 2016-2019 [Framework document integrated security 2016-2019].* Retrieved from https://www.besafe.be/sites/besafe.localhost/files/u19/2016-06-7_kadernota_integrale_veiligheid_nl.pdf.

Federation of Small Businesses (2012). *Cyber security and fraud: The impact on small businesses.* Retrieved from: http://www.fsb.org.uk/LegacySitePath/frontpage/assets/fsb_cyber_security_and%20_fraud_paper_2013.pdf.

Florêncio, D., & Herley, C. (2013). Sex, lies and cyber-crime surveys. In B. Scheier (Ed.), E*conomics of information security and privacy III* (pp. 35-54). New York, NY: Springer.

FOD Economie (2016). *Aantal actieve btw-plichtige ondernemingen volgens werknemersklasse en plaats maatschappelijke zetel, meest recente jaar* [Webpage]. Retrieved from

https://bestat.economie.fgov.be/bestat/crosstable.xhtml?view=9d19ebe2-f35a-4b51-ac1a-c153e6d77d67

Gemalto (2016). *2015: The year data breaches got personal.* Retrieved from http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf.

Goldman, R. (2016, May 12). What we know and don't know about the international cyberattack. *The New York Times*. Retrieved fromhttps://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html?_r=0

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2*, 13-20. doi:10.1007/s11416-006-0015-z

Granville, K. (2015, February 5). 9 Recent cyberattacks against big businesses. *The New York Times*. Retrieved from https://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html.

Greenfield, V., & Camm, F. (2005). *Risk management and performance in the Balkans: Support contract (MG-282-A).* Santa Monica, CA: RAND Corporation.

Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *The British Journal of Criminology, 53,* 864-885. doi: 10.1093/bjc/azt018

Heaton, P. (2010). *Hidden in plain sight: What cost-of-crime research can tell us about investing in police* [Rand Occasional Paper]. Retrieved from http://www.rand.org/pubs/occasional_papers/OP279.html.

Hewlett Packard Entreprise [HP] (2016). *HPE security research: Cyber risk report 2016.* Retrieved from https://www.thehaguesecuritydelta.com/media/com_hsd/report/57/document/4aa6-3786enw.pdf

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology, 4, 26-31.*

Kerkhofs, J., & Van Linthout, P. (2013). *Cybercrime.* Brussels, Belgium: Politeia.

Klahr, R., Amili, S., Shah, J. N., Button, M., & Wang, V. (2016). *Cyber Security Breaches Survey 2016.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G., Button, M., & Wang, V. (2017). *Cyber security breaches survey 2017.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

Kobie, N. (2013, February 12). How much does cybercrime cost the UK? Not £27bn. *Alphr.* http://www.alphr.com/blogs/2013/02/12/how-much-does-cybercrime-cost-the-uk-not-27bn.

Kopp, P., & Besson, F. (2009). A methodology to measure the impact of organised crime activities at the EU level. In E. Savona (Ed.), *Organised crime in the EU* (pp. 301-320). Rotterdam, The Netherlands: Erasmus University School of Law.

Leukfeldt, E. R., de Pauw, E., Domenie, M.M.L., & Stol, W. Ph. (2011). Oude wijn in nieuwe zakken? De aard van cybercrime en de implicaties voor de opsporingspraktijk. *Panopticon, 32,* 70-74.

Leukfeldt, E. R., Domenie, M. M. L., & Stol, W. Ph. (2009). *Verkenning cybercrime in Nederland 2009 [Exploring cybercrime in the Netherlands 2009].* Retrieved from https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/2009-09-17%20VCN2009%20DEFdef.pdf.

Leukfeldt, R., Veenstra, S., & Stol, W. (2013). High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology, 7*, 1-17.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology, 48,* 293–318. doi: 10.1093/bjc/azn001

Levi, M. (2013). *Regulating fraud: White-collar crime and the criminal process.* London, UK: Routledge.

Levi, M., Innes, M., Reuter, P., & Gundu, R. V. (2013). *The economic, financial and social impacts of organized crime in the European Union.* Brussels, Belgium: European Union.

Lipton, E., Sanger, D.E., & Shane., S. (2016, December 13). The perfect weapon: How Russian cyberpower invaded the U.S. *The New York Times.* Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region&region=top-news&WT.nav=top-news&_r=0.

Maltz, M. D. (1990). *Measuring the effectiveness of organized crime control efforts.* Chicago, IL: Office of International Criminal Justice.

Mayhew, P. (2003). *Counting the costs of crime in Australia.* Canberra, Australia: Australian Institute of Criminology.

Mayhew, P., & Van Dijk, J. (2014). International Crime Victimization Survey. In G. Bruinsma, & D. Weisburd (Eds.), *Encyclopedia of criminology and criminal justice* (pp. 2602-2614). New York, NY: Springer.

Moore, T. (2011, February 2). *Why the Cabinet Office's £27bn cyber crime cost estimate is meaningless.* Retrieved from https://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/#more-2815.

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid [A race that was never run: About cyber threats and the reinforcement of resilience].* Den Haag, The Netherlands: Rathenau Instituut.

Nationaal Cyber Security Centrum [NCSC] (2016). *Cybersecuritybeeld Nederland 2016 [Cyber security image of the Netherlands 2016].* Retrieved from http://www.ncsc.nl

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory (3rd ed.)*. New York, NY: McGraw-Hill.

Paoli, L., Adriaenssen, A. Greenfield, V.A., & Coninckx, M. (2016). Exploring definitions of serious crime in EU policy documents and academic publications: A content analysis and policy implications. *European Journal on Criminal Policy and Research.* Advance online publication. doi: 10.1007/s10610-016-9333-y

Paoli, L., & Greenfield, V. (2017). Harm: A substitute for crime or central to it? In A. Boukli, & J. Kotze (Eds.), *Zemiology: Reconnecting crime and social harm* (in preparation). London, UK: Palgrave Macmillan.

Paoli, L., & Vander Beken, T. (2014). Organized crime: A controversial concept. In L. Paoli (Ed.), *Handbook of organized crime* (pp. 13-31). New York, NY: Oxford University Press.

Paoli, L., Zoutendijk, A., & Greenfield, V. (2013). The harm of cocaine trafficking. Applying a new framework for assessment. *Journal of Drug Issues, 43,* 407-436.

Paulhus, D. L. (1984). Two-component models of socially desirable responding. *Journal of Personality and Social Psychology, 46,* 598-609. doi:10.1037/0022-3514.46.3.598

Phillips, L., & Votey, H.L. (1981). *The economics of crime control*. Beverly Hills, CA: Sage.

Ponemon (2011). *Second annual cost of cyber crime study: Benchmark study of U.S. companies.* Retrieved from http://www.ponemon.org/local/upload/file/2011_2nd_Annual_Cost_of_Cyber_Crime_Study%20.pdf

Ponemon (2015). *The cost of malware containment.* Retrieved from http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

Ponemon (2016a). 2016 *Cost of cyber crime study & the risk of business innovation.* Retrieved from http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Ponemon (2016b). 2016 *Cost of data breach study: Global analysis.* Retrieved from https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov49542

Pricewaterhouse Coopers [PwC] UK (2015). 2015 *Information security breaches survey: Technical report.* Retrieved from https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

Pricewaterhouse Coopers [PwC]. (2016a). *Information Security Breaches Survey 2016: A matter of when, not if, a breach will occur.* Retrieved from https://www.pwc.be/en/documents/media-centre/publications/2016/information-security-breaches-survey-2016.pdf

Pricewaterhouse Coopers [PwC] (2016b). *Global Economic Crime Survey 2016: Adjusting the lens on economic crime: Preparation brings opportunity back into focus*. Retrieved from https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Pricewaterhouse Coopers [PwC] Belgium (2017). *Redefining the security culture – A better way to protect your business.* Retrieved from https://www.pwc.be/en/documents/20170315-Information-security-breaches-survey.pdf

Resick, P. A. (1990). Victims of sexual assault. In A. J. Lurigio, W. G. Skogan, & R. C. Davis (Eds.), *Victims of crime: Problems, policies and programs* (pp. 69-86). London, UK: Sage.

Sen, A., (1987). The standard of living: Lecture I, concepts and critiques; The standard of living: Lecture II, lives and capabilities. In G. Hawthorn (Ed.), *The standard of living: The tanner lectures* (pp. 1-38). Cambridge, UK: Cambridge University Press.

Spalek, B. (2006). *Crime victims: Theory, policy and practice.* Basingstoke, UK: Palgrave Macmillan.

Stanko, E. A., & Hobdell, K. (1993). Assault on men: Masculinity and male victimization. *British Journal of Criminology, 33,* 400-440. doi: 10.1093/oxfordjournals.bjc.a048333

Thaler, R. (1978). A note on the value of crime control: Evidence from the property market. *Journal of Urban Economics, 5,* 137-145. doi: 10.1016/0094-1190(78)90042-6

United Nations Office on Drugs and Crime [UNODC] (2013). *Comprehensive study on cybercrime.* Vienna, Austria: United Nations Office on Drugs and Crime.

U.S. Office of Management and Budget (2003). *Circular A-4, Regulatory Analysis.* Retrieved from https://obamawhitehouse.archives.gov/omb/circulars_a004_a-4/

Van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie [High tech crime, types of crime and their perpetrators: A literature inventarisation].* Retrieved from www.wodc.nl.

Van Erp, J., Huisman, W. & Vande Walle, G. (2015). *The Routledge handbook of white-collar and corporate crime in Europe*. London, UK: Routledge.

Van Leiden, I., de Vries Robbé, E., & Ferwerda, H. (2007). *Je bedrijf of je leven: Aard en aanpak van afpersing van het bedrijfsleven [Your company or your life: Nature of and approach to extortion of businesses].* Retrieved from http://www.wodc.nl.

Van Leiden, I., Appelman, T., Van Ham, T., & Ferwerda, H. (2014). *Ondergaan of ondernemen: Ontwikkelingen in de aard en aanpak van afpersing van het bedrijfsleven [Undergo or undertake: Developments in the nature of and approach to extortion of businesses].* Retrieved from www.wodc.nl

Verizon. (2016). *2016 Data breach investigations report.* Retrieved from http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Viscusi, W. K. (2008). How to value a life. *Journal of Economics and Finance, 32,* 311-323. doi: 10.1007/s12197-008-9030-x

Viscusi, W. K., & Aldy, J.E. (2003). The value of a statistical life: A critical review of market estimates throughout the world. *The Journal of Risk and Uncertainty, 27,* 5–76. doi: 10.1023/A:1025598106257

Volz, D., & Hosenball, M. (2016, February 10). *Concerned by cyber threat, Obama seeks big increase in funding.* Retrieved from: http://www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1

Vrije Universiteit Amsterdam [VU Amsterdam], & Pricewaterhouse Coopers [PwC] (2014). *Cybercriminaliteit tegen Nederlandse organisaties: Een digitale dreiging [Cybercrime against Dutch organisations: A digital threat]* Retrieved from www.pwc.nl.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Malden, MA: Polity Press.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology, 22*(1), 45-63.

Wauters, R. (23.08.2017). *Strijd tegen cybercrime loopt mank.* De Standaard, p. 5.

Whyte, D. (2007). Victims of corporate crime. In S. Walklate (Ed.), *Handbook of victims and victimology* (pp. 446-463). Cullompton, UK: Willan.

Wickramasekera, N., Wright, J., Elsey, H., Murray, J., & Tubeuf, S. (2015). Cost of crime: A systematic review. *Journal of Criminal Justice, 43,* 218-228. doi: 10.1016/j.jcrimjus.2015.04.009

Williams, L. (2016). *Crime against businesses: Findings from the 2015 Commercial Victimisation Survey.* London: Home Office.

X (2016, February 25). Cybercriminaliteit meest voorkomende economische misdrijf in België. *Het Laatste Nieuws.* Retrieved from http://www.hln.be/hln/nl/4125/Internet/article/detail/2628148/2016/02/25/Cybercriminaliteit-meest-voorkomende-economische-misdrijf-in-Belgie.dhtml

Zerbe, W. J., & Paulhus, D. L. (1987). Socially desirable responding in organizations: A reconception. *Academy of Management Review, 12,* 250-264. doi:10.5465/AMR.1987.4307820

Zimring, F., & Hawkins, G. (1995) Incapacitation: *Penal confinement and the restraint of crime.* New York, NY: Oxford University Press.

Zinets, N. (2017, February 15). *Ukraine charges Russia with new cyber attacks on infrastructure.* Retrieved from http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN.