
# D6.1 Report on model development and adequacy of existing models and data

Deliverable submitted on 30 November 2015 in fulfillment of the requirements of the FP7 project, E-CRIME Economic Impact of Cyber Crime

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement nº607775



| | | | | |
|---|---|---|---|---|
| ecrime The Economic Impacts of Cyber Crime | E-CRIME Coordinator: Trilateral Research Consulting (TRI) | Crown House 72 Hammersmith Road London W14 8TH | T: +44 207 559 3550 | www.ecrime-project.eu |

| | |
|---|---|
| **Project Acronym** | E-CRIME |
| **Project full title** | The economic impacts of cyber crime |
| **Website** | www.ecrime-project.eu |
| **Grant Agreement #** | 607775 |
| **Funding Scheme** | FP7-SEC-2013-1 |
| **Deliverable number:** | D6.1 |
| **Title:** | Report on model development and adequacy of existing models and data |
| **Due date:** | 01/10/15 |
| **Actual submission date:** | 01/12/15 |
| **Lead contractor:** | Delft University of Technology |
| **Contact:** | Michel van Eeten |
| **Authors:** | Michael Ciere<br>Carlos Gañán<br>Michel van Eeten |
| **Reviewers:** | TRI and IPSOS |
| **Dissemination Level:** | Restricted |

# Contents

# Introduction

## 1.1 Why measure the economic impact of cybercrime?

The fact that cybercrime causes damage to our economies and societies is undisputed. Policymakers, business leaders, concerned citizens — many seek to better understand the magnitude of that damage. The E-CRIME project aims to increase that understanding, with a special focus on the impact of cybercrime on non-ICT sectors.

What is the relevance of assessing the magnitude of the impact of cybercrime? It seems mainly to serve four purposes. First, raising awareness. The magnitude can help those affected understand the gravity of the threat and the need for countermeasures. Second, improving decisions. An understanding of the impact is a necessity for making investment decisions, i.e., how much to spend on reducing the impacts as well as where to spend it. Third, assessing effectiveness of our countermeasures. If we cannot measure impacts, then it is very difficult to see if our actions are being effective. Four, guiding public policy. The overall impact on our societies is a concern of governments. A better understanding of the magnitude and evolution of these impacts helps to develop policies that reduce the overall burden on society. This is broader than law enforcement against the criminals. It also includes regulatory options, liability regimes and support structures to help businesses and citizens better protect themselves.

The E-CRIME project aims to increase our understanding of the impact of cybercrime, with a special focus on non-ICT sectors (energy, financial services, health, retail, and transport). Its two main objectives are:

1. Measure and analyze the economic impact of cybercrime on non-ICT sectors and

analyze the criminal structures and economies behind such crimes.

2. Develop concrete measures and methods to deter possible criminals and to drastically limit the attractiveness of such crimes.

This report is written in fulfilment of deliverable D6.1 "Report on model development and adequacy of existing models and data". D6.1 summarizes the key findings of the assessment on existing models explaining the economic impact of cybercrime on non-ICT sectors (Task 6.1). It also describes the E-CRIME model to assess the economic impact of cybercrime on the selected non-ICT sectors, as developed in Task 6.2.

This chapter discusses the challenge of assessing the impact of cybercrime, outlines the objective of the deliverable and the structure of the overall report.

## 1.2 How to measure the economic impact of cybercrime?

Assessing the cost of cybercrime has been turned out to be a controversial undertaking. Everyone is familiar with the attention-grabbing estimates that put the cost of cybercrime to the US economy in the order of several hundred billion of US dollars, or that estimate businesses worldwide lost more than "$1 trillion in intellectual property due to data theft and cybercrime" [85] — an estimate that was cited by U.S. president Obama and many others and which has since become an infamous example of how shoddy and biased such numbers can be.

It has proven to be attractive to capture the impact of cybercrime in a monetary amount. Such an amount is very parsimonious, we are familiar with thinking in terms of money, it seems to nicely fit the problem. We are talking about cost of cybercrime, after all, even though many of these impacts are intangible effects, like foregone efficiency gains, and not actual money being lost.

Furthermore, by using a common metric like money, the impact becomes comparable and more amenable to decision making. Policymakers can compare cybercrime with other societal problems and develop appropriate responses. Law enforcement agencies can compare it to other forms of crime and help allocate scare enforcement resources to the most urgent areas. Monetary estimates are useful for firms that want to calibrate their security investment levels through standard approaches like return-on-security investment (ROSI) or annual loss expectancy (ALE).

While the need for comprehensive monetary estimates is understandable, we argue that

E-CRIME should not generate such estimates. The core problem is that it is currently impossible to generate trustworthy monetary estimates for the impact on a country or a sector, let alone for the European Union as a whole. Some effects can be monetized based on available empirical data, but many cannot. Even where decent data is available, let say from a survey among firms of the cost of security measures, it is extremely difficult to extrapolate these impacts to higher levels of aggregation, such as all firms in a sector or the economy as a whole.

## 1.3 What is wrong with current monetary estimates?

To better understand why we should not strive for a comprehensive monetary estimate, we have to take a closer look at how such an estimate could be generated. To be clear: there is nothing intrinsically wrong with monetary estimates. The problem is that there is no viable way to put a Euro amount on the overall impact of cybercrime.

What about the estimates that circulate in media reports and policy documents? Everyone understands that some of them are mainly produced for sensationalist headlines. The infamous $1 trillion figure was published by the security company McAfee, who claimed it was based on the work of several researchers. When asked, all these researchers denied having produced the estimate and all denounced it as being invalid [80].

There are more thoughtful estimates, however, that are based on methods which are explained in a publicly-available report. One example is a 2014 report called "Net Losses: Estimating the Global Cost of Cybercrime", published by McAfee and the Center for Strategic and International Studies (CSIS) [84]. It is illustrative to dissect this specific, widely cited example, so that we can see that there really is no way to adapt such an approach for the purposes of the E-CRIME project – or for any project that cares about the validity of its estimates.

The report estimates that "the likely annual cost to the global economy from cybercrime is more than $400 billion. A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion" [84, p. 5]. The main approach of the underlying research is said to be an aggregation of existing data sources: "We calculated the likely global cost by looking at publicly available data from individual countries, buttressed by interviews with government officials and experts."

Not all of these data sources can be easily traced from the report. The ones that can be verified reveal how the approach plays out in practice. Take the issue of the cost of

data breaches. The report mentions an external source that estimates that more than 800 million individual records were lost in 2013. It goes on to state: "This alone could cost as much as $160 billion per year" [84, p. 3]. Where does this number come from? It seems to be based on an annual study by the Ponemon Institute, which includes an average amount of damage per record lost — e.g., $188 per record in the US, $199 in Germany [124]. These amounts are the outcome of a survey among 217 companies in 16 sectors in 9 countries. Let us take a closer look at that data.

It should be noted that a lot of data on the impact of cybercrime stems from surveys. These suffers from several well-known problems leading to unreliable results. "Can any faith whatever be placed in the surveys we have?" ask Florencio and Herley [46]. "No, it appears not," is their answer, after an extensive analysis of existing cybercrime surveys.

The Ponemon survey is arguably among the better ones, but the problems are still immediately clear. First of all, the damage is measured via self-reporting. It is very difficult for respondents to accurately estimate how much a breach has cost their firm. They will use different definitions of these cost, so the answers cannot be consistent and are likely to cover different impacts and effects. The respondent's errors are also prone to overestimation, as there is a hard lower limit (zero) but no such upper limit.

The second problem is that the survey has received inputs from, on average, 1.5 respondent per sector per country. So whatever one or two respondents estimate for their own firm determines the damage estimate that is recorded for the whole sector in that country. Given the heterogeneity of the firms in any sector of the economy, this cannot possibly be representative. Furthermore, each firm who reports losses might have lost very different types of data records, which might have different impacts.

Third, the sectors are also wildly different from each other. A lost record in one firm can be much more harmful than a lost record in another firm, let alone another sector. Notwithstanding all these differences, the authors of the study add up all the lost records and all the self- reported damages and then calculate an average loss per record.

What meaning can possibly be attributed to that average loss per record estimate? The short answer: not much. More recently, Verizon analyzed 200 cyberliability insurance claims where there was a data breach. Their finding was that the average loss per record was $0.56 [140]. In other words, around half a dollar. This estimate is a factor of 360 lower than the self-reported figure of around $200 from Ponemon. (Verizon also notes that the average-loss-per-record is basically a useless number, as it assumes a linear relationship between breach size and overall cost, while the data shows a non-linear relationship.)

The survey approach by Ponemon produces the average loss per record by adding up many different apples and oranges, which were already unreliable estimates to begin with. Errors are multiplied with other errors until it is unclear if any actual information remains.

The McAfee/CSIS report not only ignores all of these problems, but makes them exponentially worse by simply multiplying the average amount per record with another estimate: the total number of records that were lost across the world. The result of this cascade of error magnification is basically a random number biased towards overestimation.

In general, the 'data' that goes into estimates like those presented by McAfee and CSIS resembles a set of nested Russian dolls. Each number is derived from another number, called data. But when we open up the latter number, we find no actual measurement, but yet again an extrapolation and aggregation of a third number. This continues until we reach the final doll, which in this case is the survey responses of 217 people, who may or may not have a reasonable view of the impact on their own organisation. This impact is relatively decoupled from the number of records involved, so the average loss per record is already not really meaningful. Even if it were, it cannot possibly be used as the basis for an extrapolation of 217 people to the world economy suffering $160 billion worth of damage per year.

Another example from the McAfee/CSIS report shows the same series of Russian dolls. The authors collect "public data" from different countries on the cost of cybercrime as a percentage of GDP. For the Netherlands, they include a data point that puts the damage at a whopping 1.5% of Dutch GDP. Together with similar percentages from other countries, they calculate an average percentage of GDP, which can then be nicely — or rather: horribly — extrapolated to damage as a percentage of global GDP. Hence the figure of $400 billion as the total global cost of cybercrime.

When we open up the Russian doll of the 1.5% data point for the Netherlands, its origins are not clearly sourced, but it seems to stem from a report by the Dutch research organization TNO (see [92]); the report itself is no longer available online, for unknown reasons.) The TNO report does not include actual measurements, but is yet another extrapolation that leads us to further Russian doll. TNO took a study by the UK firm Detica and "scaled" the UK costs to the Dutch economy. Is there actual data inside the doll of the Detica study? Not really. The numbers are based on murky calculations that outsiders cannot verify and that have been widely criticized [12]. Around 60% of the total cost is attributed to intellectual property theft and espionage. How is this damage measured? It seems that the Detica authors have simply made a number of assumptions

without any empirical data. In other words, inside the final Russian doll is no actual data, just speculation.

With their insistent talk about data, these report obscure that there are only the faintest of measurement signals present in the analysis. To the degree that there is any real data in there, it is lost through a series of irresponsible extrapolations and aggregations. The final result is an estimate that has no value whatsoever. "None of these approaches are satisfactory," authors of the McAfee/CSIS report write euphemistically about their approach, "but until reporting and data collection improve, they provide a way to estimate the global cost of cybercrime and cyberespionage." Well, yes, but only if you do not care whatsoever about validity. Some numbers are worse than no number.

## 1.4 Objectives and outline of the report

This brief exploration of how the existing monetary estimates are derived demonstrates why they are at best meaningless and at worst biased disinformation. For E-CRIME, we propose a much more modest approach. Some effects we can estimate in terms of monetary amounts, others only in qualitative terms. There will not be a nice parsimonious number at the end. Validity trumps parsimony when it comes to improving our understanding and informing our decisions.

The report's objectives are:

1. Survey the adequacy of existing models and data sources to model and measure the impact of cybercrime, building on the work done by WWU in D4.1;
2. Develop a model of the economic impact of cybercrime;
3. Explore how the model elements could be measured and estimate, using existing data sources as well as the consumer survey designed and implemented in WP4 and WP5.

The remaining chapters of this report correspond to these objectives. Chapter 2 surveys the state of the art, Chapter 3 develops a model, and Chapter 4 explores if and how model elements can be measured and estimated. As a whole, the report lays the foundation for the actual estimation of the impact of cybercrime, which will be presented in D6.2.

# State-of-the-art

An earlier E-CRIME deliverable (D4.1) provides an elegant overview of a variety of available data sources, as well as their typical strengths and weaknesses. We will not repeat that analysis here. In this chapter, we explore more conceptually what data is available for generating estimates of economic impact and how these impacts can be aggregated systematically into an overall assessment of the societal impact of cybercrime.

## 2.1 Ingredients of a comprehensive assessment

We see a similar logic at work when we look at the existing assessments of the impact of cybercrime, some well-known examples of which were discussed in the previous chapter. They identify a variety of impacts, some of which are then estimated based on a certain type of empirical data. Where there is no data available these costs are not estimated. Sometimes these gaps are filled with calculations based on assumptions made by experts [34] or with some form of simulation [79].

There are also studies on the cost of cybercrime that provide parts of a comprehensive assessment. Either they focus on articulating a model to enumerate the different impacts (e.g., [78]), or on estimating only specific impacts based on a specific data set, such as data breaches (e.g., [140, 103]) or consumer losses related to malware [124].

Only a handful attempts try to do both: present a model or model to systematically identify the impacts and then use data from a variety of sources to estimate the impacts, either at the national or at the global level. There are the reports of McAfee and Detica, discussed earlier. They bring the partial estimates together into some overall monetary amount. We already argued why this approach is not one to emulate for E-CRIME.

The only alternative we know of is the study by Anderson et al. [12]. This presents a model that identifies direct, indirect and defence cost. Rather than adding up the partial estimates, they argue it is more informative to present these impacts separately.

We will take an approach similar to their, though with substantial modifications, to be discussed later in this chapter and the next. To get a sense of what is possible when estimating impact, it is useful to understand what basic forms of data can go into such studies. This clarifies the constraints under which such models or models have to operate.

Any assessment of the economic impact of cybercrime needs three core ingredients:

- Data — that is, observable events related to cybercrime, such as crime reports, data breaches or security expenditures;
- Methods to 'translate' the event into an economic impact, such as a monetary estimate or a more qualitative description like forgone efficiency gains;
- A model to systematically identify and correctly aggregate the different impacts so as to assess the overall impact to society.

In Section 2.1 to 2.6, we focus on the first ingredient: data. The second ingredient, methods to associate events with economic impacts, is not specific to cybercrime, so we will not survey those methods. We refer the interested reader to sources that provide a survey of approaches to estimate economic value [27]. The third ingredient, a model for aggregation, will be explored in Section 2.7. We discuss a variety of known and lesser-known models that have been developed to synthesize different effects and into a more comprehensive picture. We end with a brief reflection on the some of the issues with these models that need to be resolved to better estimate the impact. These issues set up the challenges for the development of our own model, which is presented in the next chapter.

First, however, we turn to the different types of empirical data — that is, observable events — that can go into cost estimates. We provide a high-level overview of the basic types of data that can go into an assessment. These types are:

- Surveys collecting self-reported impacts among consumers and organizations;
- Breach notifications provided by organizations to regulators or customers;

- Technical incident data collected by security companies and researchers via automated tools like honeypots, sandboxes, spam traps, darknets and anti-virus clients;
- Crime reports filed with law enforcement agencies;
- News reports that capture anecdotal events, sometimes with more detail.

We are not claiming this list is exhaustive, but it covers the data sources that are used in most known impact studies. There are other useful sources, of course. Insurance claims, for example, can also give a reliable view into certain types of events [93]. This data is not available, however, for independent research. Furthermore, the market for cyberinsurance is still too small to give a representative view of many different types of events.

## 2.2 Surveys among consumers and organizations

Since 1996, organisations have been conducting surveys to quantify the diversity and amount of threats that appear when using computers. These surveys vary not only on the entity that conducted them, but also on the questionnaire, the methodology, the surveyed population and the statistical techniques used to analyse the results. In turn, due to this variety of properties it would be misguided to compare the results across different surveys.

Aside from a few exceptions, surveys of cybercrime victims are often based on small, unrepresentative samples, from which the extrapolation to the wider population generates unrealistic estimates. Moreover, some other surveys do not even clarify their methodology, making it hard to assess their results (e.g. [33]) However, even methodologically robust surveys present other limitations. Some crime generic surveys only spent a few questions digging into the details of cybercrime and do not class all incidents reported related to 'negative online experiences' as cybercrime.

For many years, one of the most comprehensive survey was the one conducted by the Computer Security Institute (CSI) in association with the San Francisco Computer Crime Squad of the Federal Bureau of Investigation (FBI) in 1996 [29]. During its first run the survey was distributed to 4,971 information security professional in corporations, financial institutions, government agencies, and universities. However, only 428 questionnaires were returned (response rate of 8.6%). The main goal of this survey is to analyse important computer security trends, including: (i) unauthorised use of computer systems; (ii) the number of incidents from outside, as well as inside, an organisation; (iii) types of

attacks or misuse detected; and (iv) actions taken in response to computer intrusions. Following runs of this survey included modification in order to address emerging security issues and other type of institutions (e.g. medical institutions).

The equivalent Australian survey is produced by the Australian High Tech Crime Centre (AHTCC), in collaboration with federal, state and territory police [16]. With similar goals as the CSI/FBI survey, the Australian survey consisted of 24 questions, both closed and open ended, to ascertain: business description, types of IT security used, types of cybersecurity incidents experienced, and industry reporting of incidents. However, this survey achieved a larger response rate than the CSI/FBI survey. Of the almost 450 organisations contacted, responses were received from 255 in 2012 (response rate around 60%) and from 135 in 2013 (response rate around 30%).

Since 2009, the Ponemon Institute has been conducting surveys with the same goal but a bigger scale surveying in 252 organisations using a cross- section of industry sectors in 7 countries in 2015 [106]. Obtaining a higher number of respondents (2,128) than the previous surveys, this survey follows a different surveying methodology and instead of mailing the questionnaire, field-based research was conducted. This involved interviewing senior-level personnel about their organisations' actual cyber crime incidents. However, their sample only covered large-sized organisations Thus, as stated in the previous section, it constitutes one of the most comprehensive surveys but still suffers from clear limitations (i.e., self-reporting cost estimate and non-response bias).

The cover the gap left by the Ponemon survey, the Federation of Small Business (FSB) carried out their own survey to assess the impact of cybercrime on small businesses [42]. The survey aimed at investigating the current experience of small businesses with regard to online crime and fraud and the associated cost to business, both in monetary terms and in management time. It also tried to capture current actions taken by businesses themselves to mitigate the risk of fraud and online crime. By leveraging their survey panel which was broadly representative of the wider FSB membership, more than 2,667 members were interviewed.

Similar surveys have been generated by other consulting agencies. PwC recently published the Global State of Information Security Survey 2016 [10] based on the responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 127 countries. On a more regional scale, KPMG conducted a survey on the impact of cybercrime in India [77], while Deloitte survey aim at quantifying the financial impact and total cost of cybercrime to businesses in Ireland [33].

Another group of cost estimates have been generated by security vendors, e.g., Kasper-

sky [74], Symantec [125] and McAfee [84]. For the last 5 years, Kaspersky has conducted a survey to collect insights from IT professionals about IT security risks. In the 2015 edition, the survey covered 5,564 respondents across 38 countries all IT professionals. Similarly, Symantec has been collecting data on Internet threats for the two decades. However, their surveyed population is completely different. Symantec not only covers IT professional but anyone that could be a victim of cybercrime. In 2013, 13,022 adults were interviewed across 24 countries.

| Title | Author | Year | Country | # Respondents | Response Rate |
|---|---|---|---|---|---|
| Computer Crime and Security Survey [30] | CSI/FBI | 1996 | US | 428 | 8.6% |
| Cyber Crime and Security Survey [16] | CERT Australia | 2013 | AU | 135 | ~30% |
| Cost of Cyber Crime [106] | Ponemon Institute | 2014 | US, UK, DE, AU, JP, FR, RU | 2,081 | - |
| Cyber security and fraud: The impact on small businesses [42] | Federation of small businesses | 2013 | UK | 2,667 | 41% |
| Cybercrime Report [125] | Norton/Symantec | 2015 | AU, BR, CA, CO, DE, FR, DE, IN, IT, JP, MX, NL, NZ, PL, RU, SA, SG, SA, SW, TR, UA, UK, US | 13,022 | - |
| Economic Cost of Cybercrime in Nigeria | Paradigm Initiative Nigeria | 2013 | NI | 2,980 | - |
| Irish Information Security and Cybercrime Survey [33] | Deloitte | 2013 | IR | 60 | - |
| Cybercrime survey report 2014 [77] | KPMG | 2014 | IN | 170 | - |
| Global Economic Crime Survey [10] | PwC | 2014 | Global (127 countries) | >10,000 | - |
| Global IT Security Risks Survey [74] | Kaspersky Lab | 2015 | Global (38 countries) | 5,564 | - |

## 2.3 Breach notifications

In the past decade, a variety of regulatory regimes have emerged that require organizations to report data breaches when certain conditions are met. The underlying assumption is that one cannot expect businesses to be proactive in revealing their failure to secure sensitive data; such a revelation can harm a business's reputation and destroy the trust of their customers. The laws are meant to overcome this incentive problem and force organisations to be transparent about data breaches.

The US has been leading: in 2003, the state of California introduced the first *Security Breach Notification Law* (SBNL). This SBNL, according to the official text, "[...] would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation." [117]. Most other states in the US followed with SBNLs based on the Californian example. There are however some differences in the legal details, such as what penalty follows when a company fails to comply, and possible exemptions, such as when the breached data is encrypted. Joerling [71] provides an overview. In addition to state-level laws there is sector-level regulation in some sectors. Unsurprisingly there is especially stringent regulation in sectors where sensitive data is critical to doing business, like the financial sector and the health care sector.

These SBNLs have led to many notifications of data breach incidents. One of the most-used repositories of this data is the Privacy Rights Clearinghouse (PRC) [50], a nonprofit organisation that accumulates data breach reports from several sources, including news reports, voluntary submissions by notified consumers, and government documents acquired using the Freedom of Information Act. This dataset starts in May 2005 and now includes over 4,600 reported data breaches. It is important to note that not all mandatory notifications are public by nature. In some cases, only directly affected consumers receive a notification. The PRC depends on consumers to submit these notifications to ensure it also captures those breach events.

Following the US example, the European Commission presented the Network and Information Security (NIS) Directive in 2013, to tackle network and information security incidents (European Commission, 2013). The NIS Directive is close to being finalized.

Once it is in place, countryâĂŹs will be required to set up their own notification regimes. This is likely to lead to inconsistent criteria and practices for notifications. It seems that the directive also allows for the notifications to be made confidentially, in which case the E.U. would not capture the benefits of building a public dataset of breaches that can be studied and used to evaluate policies and risk assessment.

Despite regulatory efforts, it is generally believed that data breaches are still underreported [94]. The magnitude of underreporting is unknown, but it is likely to be significant. Organizations may not always be aware a breach has occurred. It is also not fully clear when the legal threshold is met for breaches to require notification. Does there need to be proof of active extraction of personal information, for example? Given the incentives we mentioned earlier, organizations are likely to behave strategically when deciding whether to notify or not. One study found the remarkable pattern in health care organizations: the number of breach notifications went up after the sector adopted more encryption of patient records [89]. This seems puzzling, but one explanation could be that medical organizations are more willing to report breaches when they use encryption, because the consequences of the loss — and thus of the notification of that loss — are less severe. This suggests strategic behavior: the more severe the consequences, the stronger the incentive not to notify. That being said, it seems likely that larger breaches are more difficult to hide, as others might observe this data being abused, for example via fraudulent credit card transactions that can be correlated to a certain retail chain.

There has been research trying to estimate the business impact of data breaches. Cavusoglu et al. [24] found that the stock market value of companies dropped after the publication of their security breaches, an effect that was disputed by Campbell et al. [23]. More recent estimates have been developed by industry, most notably Verizon [140]. Their yearly report includes many more breach events than those covered by PRC, data that Verizon get via collaboration with a network of partners. They also include useful cost estimates based on 200 cyberliability insurance claims following data breaches. This data is supplied by NetDiligence, which is a risk assessment firm working with major insurance underwriters [93].

## 2.4 Technical incident data

Security companies and academic researchers studying cybercrime have develop a wealth of tools to observe security incidents. These are the data sources that underlie most of the reports on cybercrime trends published by security companies. We summarise the main tools here and refer to examples of reports based on them. Please note that most

referenced industry reports include data from multiple tools on our list, thereby covering a variety of attack trends.

- Spam traps are essentially mailboxes set up for the sole purposes of being targeted by spam. By looking at what is received in the traps, one can study trends in the volume and nature of spam distribution and email phishing attacks [136, 132].

- Honeypots are computers set up to be discovered and compromised by attackers, which allows the research to study attack patterns and malware evolution. It is one of the ways in which new malware variants are discovered. It also helps to discover the criminal resources used to communicate with the compromised machines, like URLs and IP addresses that host command-and-control servers. Those can be added to blacklists that block access to these resources to protect users [1].

- Sinkholes are the systems put in place after defenders have wrestled control over a botnet, a network of compromised computers, from the criminal masters. The sinkhole replaces the criminal command-and-control servers and as such it sees all the compromised machines of that botnet reporting in for new commands. It helps to measure how many machines have been victimised by a certain botnet. Some resources of sinkhole data are disseminated to ISPS to facilitate cleanup of their customers [7].

- Crawlers are the tools that underlie search engines and other indexes of Internet resources. It is basically a software programs that analyze the content of web pages or other types of resources, and then follows all the links it finds in that resource, then in turn analyses all those resources and follows all the links from those, et cetera. In this process, it can also discover malicious resources, such as sites that try to download malware to the visitor or that present phishing pages to capture account credentials. This kind of information can be used to build blacklists to protect users by blocking access to these pages or resources. Think of the Google Safe Browsing tool, which helps protect users of Google search and the Chrome browser [53].

- Darknets are machines that receive traffic at IP addresses that are not officially in use. Some of this traffic comes from attackers scanning the Internet for vulnerable devices. It can help track what kind of tactics attackers are using to find victims, as well as the volume of such attempts [66].

- Intrusion detection systems, like firewalls, can collect log certain events, for example, connection attempts from outside the network to systems inside the network. Some of these attempts might be seen as non-legitimate traffic and they might

point to trends in the volume and evolution of attacker tactics. There are data sources that aggregate these logs from firewalls deployed at different organisation across the Internet [69].

- Darkweb monitors are different types of tools to track activity in criminal marketplaces, often hidden inside the anonymising Tor network, like the infamous and now defunct Silk Road. By studying what is offered and at what prices, one can get a sense of criminal trends and business models [135].

- Anti-virus clients and malware removal tools run on millions of consumer and business machines and can report which type of malware has been encountered or cleaned-up [125]. One of the largest data sources of this type is the telemetry collected by Microsoft via its Malicious Software Removal Tool. This tool runs every month on all Windows machines that install automatic updates. According to Microsoft, it receives data from more than 600 million machines worldwide. Together with other data sources, this allows the company to track trends in different types of cybercrime in their Security Intelligence Reports [13].

- DDoS mitigation tools are deployed in the networks of customers of the security companies that offer these tools. From this viewpoint, the security company can collect data on attack volume, trends, origins and targets [139, 64].

These kinds of data sources can be quite helpful in assessing the impact of cybercrime, but we need to keep in mind several limitations.

The first, and perhaps most important, limitation is that these tools are mostly suited to track attacker trends, rather than the actual impact. Take phishing. The fact that the volume of phishing attacks increase can mean two things: either more people fall victim to these attacks or the attackers are increasing the volume in response to lower success rates and because they are competing with other attackers [88]. Another example is financial fraud. In 2012, McAfee reported on uncovering operation "High Roller", which stole money through malware-based takeover of financial accounts. McAfee reported that "the total attempted fraud could be as high as €2 billion" [82]. Notice the word "attempted". It is a half-hearted acknowledgment that in reality the security firm has no way of knowing how much was actually stolen. In response to this report, Dutch banks commented that the losses they saw were less than 10 percent of the amount reported by McAfee. In other words, they were able to stop more than 90 percent of the fraudulent transfers observed by McAfee before they became irreversible. So the numbers were potentially over-estimating the cost by one order of magnitude.

These examples point to the general discrepancy between measuring attacker activity and

measuring the effectiveness of those activities. The sources used in security intelligence reports are strong in the first and weak in the latter. Of course, the latter is crucial if we are to base impact estimates on these numbers.

Other limitations are more practical. Many sources, especially those of commercial vendors, are inaccessible for independent research. That makes it difficult to use them for impact assessment, unless one is willing to simply trust the aggregate statistics that can be gathered from the public reports.

A last limitation to discuss is that these sources only contain partial and biased views of the problem. The commercial reports rarely reflect on issues of bias. In academic studies, this is more prevalent. The upshot is that bias can lead similar types of data sources to produce very different results. Another issue is that the partial view means a lot of incidents are unobserved. A comparison of more than 80 blacklists, covering several different sources on our list, found that most pair-wise comparisons of these blacklists reveal virtually no overlap (less than one percent, in most cases) [87]. This means that any single blacklist will give a very limited and potentially skewed picture of the trends.

## 2.5 Crime reports

The lack of reliable data on cybercrime offenses has been noted for some time. Back in 1989, the Law Commission for England and Wales pointed out the necessity to enforce legislative action to diminish 'computer misuse' but the insufficient evidence of the scale and consequences of cybercrime hindered its prompt development [141]. More than twenty years on and the situation has not improved greatly [12]. Although simple cybercrime statistics currently exist, there are a number of limitations, quirks and caveats that prevent the generation of accurate cost estimates. Some of the main challenges in improving the cost estimates of cybercrime are as follows:

- Lack of consensus as to the meaning of 'cybercrime': when there is not a universal definition of 'cybercrime', official crime statistics will depend on what is considered as cybercrime and what is not. Even where there is a specific cybercrime, it may be concealed within other statistics [75]. For instance, unauthorised access to a data server under the Computer Misuse Act [142] is computed as 'other fraud' in the Crime Survey for England and Wales [59]. Similarly, the 2012 report by the Congressional Research Service [45] stated that just as there is no overarching definition for cybercrime, there is no single agency that has been designated as

the lead investigative agency for combating cybercrime.

- Misclassification of IT-related offences as cybercrimes: while an offence itself, such as stalking, is recorded in crime statistics, the use of technology by offenders may not. However, current policies on how to differentiate and incorporate the use of computers within crime statistics are not yet mature. For instance, the US Uniform Crime Reporting Program allows crime officers to indicate whether a computer was the object of the crime or was used to perpetrate the crime [83]. While this is a useful development, it may skew results as theft of electronic appliances (e.g. laptops, tablets, mobile phones, etc.) is therefore included within 'computer crime' statistics.

- Reported cybercrimes may not accurately reflect the level of actual offending: under-reporting of both cyber-dependent and cyber-enabled crimes is an issue amongst the general public and businesses. According to the 2013 UK Cyber crime report [86], two per cent of online crime incidents were reported to the police by businesses. Similarly, the Crime Survey for England and Wales [76], just 1 per cent of adult internet users who experienced hacking or unauthorised access to their data in the 12 months prior to the survey reported this to the police not report attacks to any external party. There are several reasons behind under-reporting [86]: (i) perceptions that the police will not/cannot do anything about online crimes; (ii) not knowing where to report; (iii) porting to other bodies such as banks or internet service providers; (iv) perceptions that cybercrimes are not 'real' crimes like, for example, vehicle theft or burglary; (v) victims not realising or perceiving themselves as victims, for example, because a bank has refunded lost money, or being unaware that malware has infected their computer and stolen their personal details; and some victims simply being too embarrassed to come forward, for example, regarding common scams.

## 2.6 News reports

The data sources we discussed above cover the main inputs for a systematic estimate of economic impacts. We would be remiss, however, if we did not also acknowledge that news reports can also provide useful insights. While anecdotal by definition, news organisation occasionally uncover breaches — or more likely: receive tips about breaches — that otherwise would go unnoticed. Take the Sony attack. Not only did the media bring this into the spotlight, the follow-up coverage gave the public quite some details about the kind of fallout that the company suffered from the attack.

Databases of news reports can be queried to look for certain events or trends. Of course, known biases in reporting have to be kept in mind. Media reporting of cybercrime may present a distorted picture and the impact of cybercrime may be uncritically inflated. The focus is typically on the most spectacular and therefore rare events, rather than the most frequent or impactful [143, 12].

## 2.7 Models for aggregation

When one or more data sources of the types discussed above are available, one faces the next problem: aggregation. Any measurement instrument captures only a specific class of events that the instrument can observe. This generates two challenges: generalisation and aggregation.

Generalisation concerns the issue of getting from the observed events and their impacts to an estimate of all events of that type and their impacts. Surveys of financial losses by organisations can be particularly challenging to interpret, in this respect, as they always deal with a small number of data points in relation to what they are supposed to represent: all organisations.

As outlined by Florêncio and Herley [46], many of the survey-based estimates of losses are driven by the inclusion of high-value single outliers, which heavily skew and exaggerate results. A handful of respondents formulate the majority of the estimate. This can then lead to unreliable generalisation of findings to the wider population. This is key explanation for why some estimates differ by several orders of magnitude.For instance, according to the Internet Crime Complaint Center, in 2010, Internet crime loss by individuals totalled $560 million [68] in the US alone, while McAfee estimated a $1 trillion global cost [73].

The second issue is aggregation. Even when generalisation is performed satisfactorily, it only results in a total estimate for a specific type of impacts. For example, a survey among firms can only yield firm-level impacts. It does not take consumers-impacts into account, the cost of law enforcement, and many other effects. Remarkably many studies ignore this issue and are rightly criticised for it [12, 46, 122, 112]. They simply extrapolate firm-level losses to estimate the overall loss to society. But many of the firm-level losses are not losses to society. Think of a firm that loses customers due to reputation damage after a breach. Those customers will likely go to another firm. In other words, this is no net loss, only a transfer of wealth among firms.

There is a need for a model that can identify and systematically aggregate these different impacts into a comprehensive assessment. In table 2.7, we list publications that provide such models or reflect on these issues of generalisation and aggregation.

In the next Chapter, when we will set up our own model, we will take elements from these earlier studies, especially from Anderson et al. [12], but also make certain adaptations.

First of all, we think that the current situation of limited and partial data on many cost impacts is a constraint that will persist for the coming years. In principle, one could envision better and larger surveys among firms, but self-reporting economic impacts will remain very difficult for respondents. Furthermore, even larger surveys, letâĂŹs say among thousands of firms, will not solve the issue of generalising from them to the larger aggregates of sectors, let alone countries or the world. Even a single sector in a single country harbours a large heterogeneity that would need large samples to accurate capture.

Other data sources present other constraints that are equally persistent. Measurement of attacker behaviour might be able to keep up with adapting attackers, but they will never measure the actual effectiveness of attacks, let alone their impact. Breach reporting will become a broader practice, certainly in the E.U, but this approach will function similar to how it is functioning now in the U.S.

For the model, this means that it has to be able to work under the existing constraints of available data. We think the model of Anderson et al. deals relatively well with these constraints. We follow their approach in enumerating and estimating a number of impacts. We also follow their lead to purposefully not generate an overall monetary estimate. Our model, like theirs, will aggregate by bringing different impacts together in a systematic way, but not by adding up the different partial estimates. It would be uninformative, as some impact cannot be estimate quantitatively and the largest quantitative impacts would overwhelm all others. Also such an aggregation would be potentially misleading, since the partial estimates all have different uncertainties and confidence levels associated with them.

We will, however, also make certain adaptations. The most important departure from their approach, and from the other existing models, is that we will distinguish more precisely between agent-level impacts (i.e., firm, organisation, consumer) and societal impacts. All existing models treat the overall societal impacts as the accumulation of agent-level impacts. As we will discuss in the next Chapter, some costs to organisations are not societal losses, but rather wealth transfers of one organisation to another. A simple example is customer churn after disclosing a data breach. This is a cost to

the affected organisation, but a gain to its competitors, who will receive the defecting customers. This can therefore not be consider a loss at the level of society as a whole. We will argue that the actual costs to society should not include wealth transfers but opportunity costs generated by cybercrime.

This different starting point also means we have to adapt the taxonomy of cost impacts that the model needs to articulate. Rather than following the set of impacts that Anderson et al. identified, we will use an approach similar to theirs, namely the classic distinction from the economics of crime between anticipation, consequence, and response, to systematically identify the different opportunity costs that are incurred by organisations who suffer from the consequences of cybercrime. The next Chapter outlines the model in more detail.

| Title | Author | Year |
|---|---|---|
| Estimating the Global Cost of Cybercrime [84] | McAfee | 2013-2014 |
| The cost of cyber crime [34] | Detica and Office, Cabinet | 2011 |
| Measuring the Cost of Cybercrime [12] | Anderson et al. | 2013 |
| Sex, Lies and Cyber-crime Surveys [46] | Florêncio and Herley | 2011 |
| Cybercrime: it's serious, but exactly how serious? [61] | Hyman | 2013 |
| A Closer Look at Information Security Costs [22] | Brecht and Nowey | 2012 |
| The Use, Misuse, and Abuse of Statistics in Information Security Research [112] | Ryan et al. | 2003 |
| Internet and computer related crime: Economic and other harms to organizational entities [111] | Roche | 2007 |
| A multi-level approach to understanding the impact of cyber crime on the financial sector [78] | Lagazio et al. | 2014 |
| Damages from internet security incidents: A framework and toolkit for assessing the economic costs of security breaches [138] | van Eeten et al. | 2009 |

# Economic model

## 3.1 A model for the economic impact of cybercrime

In this part of this intermediate report we introduce a model for studying the economic impact of cybercrime. This model brings together the various costs of cybercrime at different levels of society, and does so while adhering to economic principles. We believe a short review of these principles is in order, since previous cost-of-crime studies have routinely violated them. These violations are typically the result of the many complexities and problems associated with assessing the economic impact on our societies, as discussed in Chapter 2. In some cases, however, these basic principles might have been purposefully overlooked in an attempt to inflate the impact of cybercrime.

## 3.2 Economic principles and foundations

As Dorr and Simpson pointed out in their 1931 Report on the cost of crime, estimating the economic impact of crime is an exercise in imagination [35]. The effect of crime on a nation's total income, for instance, is the difference between the nation's current income and the income it would have were there no crime. To estimate this difference, one must first visualise this alternate world free of crime, and then determine how much more productive its economy would be.

Although written over 85 years ago — probably with a mechanical typewriter — the words of Dorr and Simpson have aged well and apply to cybercrime like any other crime. Cybercrime is so entwined with IT that it seems impossible to imagine a world without it, and thus no estimate of the total cost of cybercrime could possibly be accurate. It

is fair to assume, for instance, that fear of cybercrime has slowed down innovation and adoption of IT solutions, but expressing this loss as a percentage of national product seems beyond the grasp of our scientific methodologies. Nevertheless, studying the various effects of cybercrime on the economy can be worthwhile if one avoids indulging in overly-specific monetary estimates and instead aims at understanding.

Our work begins with unfolding the impact of cybercrime in two dimensions: (1) the various types of costs, classified by their relation to actual cybercrime incidents, and (2) the economic agents and entities that bear these costs. We then look into how these immediate costs bring about long term economic distortions. This gives us a model that effectively breaks down the problem of estimating the impact of cybercrime into smaller subproblems which are more amenable to detailed analysis.

In developing our model we draw upon a century of research on the cost of crime. While cybercrime is a modern invention, set apart from traditional crime in such matters as its highly transboundary character and the problems of attribution, analysing its impact requires the same economic ideas. Indeed, some of the fallacies and methodological difficulties that tainted previous reports on the costs of cybercrime were already pointed out by criminologists Hawkins and Waller [57], some 80 years ago. What follows now is a short review of several relevant principles of economics.

### Opportunity costs

The premise behind all economic analysis is that our wants are endless, while resources are scarce. Economic theory deals with the question of how to allocate these resources so as to maximise welfare.

Cybercrime poses a cost to the economy to the extent that it leads to inefficient allocation of resources. In contrast to crimes like robbery and arson, cybercrime rarely leads to a direct waste of natural resources, capital, or human life. It has however unleashed a continuing war between attackers and defenders, diverting the time and skills in law enforcement, software development and business management from more productive uses. The market for security software — with an estimated €20 million revenue in 2014 [119] — is evidence of this: the resources poured into these products could also be used to develop new technology, if there were no cybercrime.

The cost of such unproductive use of resources is measured by the foregone value of the ideal alternative — the *opportunity cost*. Quantifying such costs is not trivial. In the case of the security industry, the expended resources would arguably be most productive

if they were put towards developing new IT solutions. Since that would require mostly the same skills and investments, the current market value of the security industry gives an impression of the foregone benefits.

Often a greater deal of speculation is required. For instance, to estimate the opportunity cost of a person choosing a career in cyber crime, one has to wonder what alternative career this person is giving up. If Mark Zuckerberg had taken up click fraud in his youth, he might have succeeded in extracting a few thousand euro from the public, but the opportunity cost would have been enormous.

Engaging in such speculation is probably not the most productive use of a researcher's time, while a shallower focus on estimating observable losses and expenses is likely to result in useful illustrative figures. Nevertheless, the concept of opportunity costs serves to remind us that the ultimate cost of cyber crime to society goes beyond a simple list of losses and expenses — a point that we will return to later in this chapter.

### Wealth transfers

Opportunity costs must not be confused with *transfers of wealth*. The latter class includes any expense or loss from one party to another, which is not always an economic cost to society as a whole. For instance, a company that suffers a data breach is sometimes forced to pay a fine to some regulatory agency, and while this is a cost to the company, it is merely a transfer of wealth. Since no resources are wasted, it is not clear that society is economically worse off because of this transaction.

Many costs of cybercrime as identified in earlier studies are costs incurred by individual economic actors, not society as a whole. They belong to this class of wealth transfers. Besides direct financial transactions, this also includes effects like losing customers due to a data breach — a cost to one company, but a gain to others.

Huygen et al. [60] studied the cost of digital piracy in the Netherlands and made the case that piracy is a transfer of wealth from producers to consumers. They quantified the benefits to consumers using a welfare economics approach and convincingly showed that these benefits outweighed the turnover losses to producers by two to one, thus indicating a net gain to society, despite the losses to producers.

Although both opportunity costs and wealth transfers can be expressed in monetary units, these two types of costs are in general not commensurable; that is, they can not be added together or compared in any way. Several investigators of cost-of-cybercrime studies have

failed to understand this, and estimated the total societal impact of cybercrime by adding up individual costs. Such procedure is impermissible, and often leads to double counting problems.

An example of double counting is to first estimate the average costs of customer attrition after a data breach, and then extrapolate this number to get the costs of lost business to a whole sector or country. The error here is to forget that defecting customers usually take their business elsewhere; that is, many companies *gain* customers when one of their competitors suffer a data breach. This is essentially just transferred wealth.

## Aggregating costs

It seems callous to say that transferred wealth is not lost and therefore irrelevant to society. Indeed it would be interesting to see the burden of cyber crime on businesses, households, and government, in terms of observable losses and expenses. Yet the question remains how one can take these individual losses and expenses and aggregate them to some figure of the total cost to society.

The difficulty with such an aggregation is that the monetary quantities used to express different costs do not always refer to the same thing. To see this, we must remind ourselves of Adam Smith's observation that "it is not for its own sake that men desire money, but for the sake of what they can purchase with it." The cost of cyber crime to the household, when expressed as a monetary amount, represents the current market value of the additional goods and services it could purchase if it were immune to cyber crime. To government, the expenditure on law enforcement constitutes a share of the tax revenue, which can be interpreted as taking away from other government spending or as a virtual tax increase. To the business, the monetary sum said to be the cost of cyber crime symbolises the extra profit it could make if it were immune to cyber crime, while producing the same amount of goods and services. Finally, to society as a whole, the costs of cyber crime are perhaps best measured by a decrease in aggregate production, expressed as a percentage of GDP.

Even though these costs can all be expressed as monetary sums, they are not measured on the same scale, and they are not commensurable. Individual economic agents act in their own private interests, and the cost that cyber crime brings upon them is measured by the extent to which it thwarts those interests. Granted, by regarding their own interests — to paraphrase Adam Smith once again — individual agents often promote the public interest unintentionally, as if led by an invisible hand — but this does not mean that we can equate the interests or costs of individual agents with those of society as a whole.

Furthermore, because of this mismatch between private and public interests, individual agents may change their economic behaviour in response to the strain of cyber crime. For instance, consumers may avoid online services like banking and shopping for fear of cyber crime. Likewise, businesses may invest less in research and development, thinking that hackers would steal their innovations. The economic inefficiencies introduced by such behavioural changes form part of the costs to society.

We conclude that to understand the long term economic impact of cyber crime, one must do two things: (1) identify any irreversible waste of resources induced by cyber crime, and (2) understand the effect of cyber crime on the behaviour of individual economic agents and how this leads to economic inefficiencies.

In our model we separate the measurable losses and expenses to individual economic agents from the more structural distortions that cyber crime brings upon the economy. Practically speaking, this separation means that we first study observable losses and expenses and focus on estimating them precisely, without worrying about average or total costs to a whole sector or nation. These estimated quantities can then be used as input for more speculative analyses of long term economic impact.

Our next step is to identify the different economic agents and entities that suffer from cyber crime. Following that we classify the expenses and losses they suffer individually. We then discuss the long term economic distortions that these effects bring upon sectors, nations, and Europe as a whole.

## 3.3 Key economic agents

Our model includes various societal agents and entities that experience cybercrime. For reasons stated before, looking at their different perspectives is essential to properly understanding how cybercrime affects the economy.

**Consumers** Individual persons in their capacity as users or buyers of goods and services. When we talk about the costs of cybercrime to consumers, we mean the costs associated with crimes that individuals directly, such as ransomware or online counterfeit fraud, but not the costs they suffer indirectly as members of society.

**Businesses** Any organisation active in buying and selling goods or services. We will focus on businesses in five sectors: retail, healthcare, energy, financial services, and transportation.

We use the term *sector* loosely to refer to all organisations of similar type; sectors are not isolated segments of the economy. In fact, businesses from different sectors work closely together. E-commerce, for instance, combines the services of retailers, IT infrastructure providers, financial service companies, and logistics companies to sell and deliver goods to consumers.

The network of organisations involved in creating and selling a specific product or service is often called a *supply chain*. It is sometimes interesting to study the resilience of a supply chain to cyber crime. A cyber attack on one supplier can disrupt the entire supply chain, which creates dependencies and spill-over effects.

**IT infrastructure providers** Under this heading we include software vendors, ISPs, and cyber security providers. These organisations facilitate the use of IT systems and are thus part of any supply chain. They suffer part of the costs of cyber crime themselves, and through dependencies and externalities they play an important role in the overall impact on sectors and nations.

**Law enforcement** Cyber crime takes up time and resources of police, prosecutors, courts, and correctional systems.

**Cybercriminals** Although it may seem counter-intuitive, some of the costs of cyber-crime are borne by the offenders themselves. When a cyber criminal is sentenced to prison, this causes psychological and financial damage to the offender, as well as to his or her family. This damage may continue even after this person is released, when a criminal record makes it hard to find employment and rebuild a life.

Whether this punishment is fair or beneficial to society is not of interest; such moral judgements have no place in an economic analysis. For all intents and purposes we consider cybercriminals to be members of society, and likewise we make no distinction between a legal and illegal economy.

Including these costs makes our model more useful for policy analysis. To illustrate, it is conceivable that a more powerful justice system could deter potential cyber criminals from offending, and encourage them to pursue alternative lines of work that are more productive to society — it seems unlikely that all, or even most, cybercriminals would switch to traditional crimes such as arson or robbery. This is a potential benefit of investments in law enforcement, and as such these costs should not be ignored.

## 3.4 Costs of cybercrime to individual agents

We proceed now by listing the various costs of cyber crime to individual economic agents. We classify them as either costs in *anticipation* of cybercrime, costs as a *consequence* of cybercrime incidents, or costs of *response* to cybercrime. This categorisation emphasises the relation of costs to actual incidents. The same classification was used in several cost-of-crime studies, e.g. Brand and Price [19] and Czabanski [32]. Our typology of costs as a consequence of cyber crime incidents closely resembles earlier work by van Eeten et al. [138].

Again, these cost types should not be interpreted as the ultimate economic costs to society as whole. They merely represent the experience of individual economic agents in terms of damages, losses, and expenses. The actual long term costs of cyber crime for sectors or nations depends on how these immediate effects translate into systematic misallocation or waste of resources. We will discuss such economic implications shortly.

### Anticipation

- **Expenditure on security services and products.** This includes commercial security products, such as antivirus software, firewalls, intrusion detection systems, and smart card authentication systems, but also services, such as staff awareness training.

- **Productivity losses due to security policies.** Many security products or policies are an inconvenience to users. For instance, anti-virus software may require a reboot after an update. This presents a cost to both businesses and consumers. The same is true for encryption methods, since they take time to operate.

  Further productivity losses may arise from policies that restrict or limit access to sensitive systems. Such policies reduce operational efficiency. In the most extreme case, businesses may isolate some devices in their network (air-gapping), meaning that they can only be accessed by people in the same room. Although such costs are hard to estimate precisely, it is clear that restrictive security policies can mitigate the productivity gains desired from IT solutions.

- **Costs of security assessments.** For many businesses, cyber security risks are board-level issues. As such, business decisions may require an assessment of the associated cyber security risks.

  These assessments may take the form of quantitative risk estimations or more

qualitative sign-off procedures. This may happen informally or performed by designated Information Risk Management units or Security and Safety departments. Security may also play a role in due diligence in mergers and acquisitions or in procurement procedures. These assessments take up time and resources and delay developments.

- **Insurance costs** Some insurers offer policies that cover the costs resulting from data breaches or online banking fraud. The premiums that businesses pay for these policies are costs in anticipation of cyber crime. These premiums are partly returned to policy holders in the form of claim payments, but some of it is lost to the overhead costs of the insurer.

- **Cost of awareness initiatives.** Governments or trade bodies sometimes lunch initiatives to raise awareness on cyber security risks. These initiatives include TV commercials that warn consumers against phishing (like the Safe Banking campaign by the Dutch Payments Association) and websites with information on safe Internet use (like www.getsafeonline.org in the UK). Naturally, such initiatives take time and resources to launch and maintain.

### Consequence

- **Stolen funds.** This includes all forms of directly stolen funds by means of fraud or identity theft.

- **Pain and Suffering.** An umbrella term commonly used in cost-of-crime materials to refer to any reduction in quality of life set on by incidents. This includes any emotional distress brought on by cyber crime incidents.

  Pain and suffering is a cost in and of itself, in the sense that it diminishes well-being — although one could argue that an economic analysis should focus solely on economic welfare. It also may cause individuals to be less productive in their working life, or have other secondary effects. This category does however not include the cost of behavioural changes set on by emotional distress, like avoidance of online services.

  In materials on the costs of crime there seems to be a consensus that quantifying the effects of pain and suffering is infeasible. We believe that cybercrime is no exception. If we were to analyse a case of identity theft, for instance, we should not attempt to quantify the feelings of violation and frustration and get a euro amount that we can add to the direct financial losses from the incident; such an exercise is unlikely to be of any value. As such these costs cannot be part

of cost-effectiveness calculations, but they could play a role in more qualitative cost-benefit analyses, if one is willing to work with different types of costs.

- **Cost of disruption**

  Cyber attacks can have a disruptive effect on business processes. This is true for all cyber attacks, in some sense, but especially for denial-or-service attacks, malware, or spam. Consumers, on a smaller scale, may also suffer from disruptive attacks.

  These disruptions lead to productivity losses and missed sales for businesses, and often have spill-over effects on organisations in the same supply chain.

  In this category we do not include the costs associated with recovering from an attack and restoring normal operations.

- **Repair costs** All costs borne in restoring the availability, integrity and confidentiality of compromised systems. This includes anything from removing malware to resetting account credentials.

- **Reputation damage and customer attrition** For businesses, publicised cyber security breaches may lead to reputation damage and loss of trust. This may result in a loss of customers. The cost of such reputation damage mostly consists of the lost market share and the expenses on public relations measures.

- **Loss of intellectual property and trade secrets** Businesses may lose a competitive advantage if the confidentiality of sensitive data is breached. This sensitive information could be anything from a technological design or a secret recipe to internal communication about an impending business deal.

  As explained aptly by Anderson et al. [12], the cost of such compromise only takes shape if some other party desires and succeeds to exploit the information, which is often not trivial. Intellectual property is protected by copyright or patent laws, which means that ill-intending parties cannot easily exploit the stolen information. Financial markets have mechanisms to detect insider trading. Nevertheless, there are many conceivable scenarios in which a business or nation suffers from theft of intellectual property or trade secrets.

### Response

- **Law enforcement.** All costs made by the criminal justice system — police, prosecutors, courts, and the correctional system — in fighting against cyber crime. Also included are costs for witnesses and suspects.

- **Effects on offenders.** Offenders of cyber crime give up potentially lucrative career paths; Herley and Florêncio [58] explained why cyber crime is often barely profitable. In addition, offenders may get prosecuted and sentenced.

- **CSIRTs.** Computer Security Incident Response Teams (sometimes called Compute Emergency Response Teams or similar variants) are teams that coordinate the response to security threats. These teams exist in both the private and public sector. Over the years, CSIRTs have expanded their services from incident response to include precautionary services and as well, such as vulnerability analysis and awareness building.

  According to ENISA[1] there are over 100 CSIRTs in Europe.

## 3.5 Economic and social impact

The costs listed above characterise the burden that cyber crime puts on individual economic agents in terms of losses and expenses. In this section we investigate the long term implications of this burden on the economy of a nation or sector. Our focus is on implications for non-ICT sectors.

### Consumer avoidance

Cyber crime may cause consumers may avoid using services such as online banking or online shopping. This avoidance could be the result of a levelheaded consideration of the risks or the result of a more general sense of fear and discomfort in anticipation of crimes like fraud or identity theft. Either way, this avoidance effect undermines some of the potential economic efficiencies brought about by online services. These efficiencies include the lower transaction costs of online payments and the reduced search costs in online shopping [49].

### Market frictions and inefficiencies

The costs of cyber crime to businesses, as enumerated in the previous section, in effect represent a reduction in productivity; that is, businesses need more inputs to produce the same output, because time and resources are wasted in the production process. This

[1] the European Union Agency for Network and Information Security

leads to higher market prices, which distorts market supply and demand and brings about efficiency losses.

One might consider the sum of extra inputs required to produce one unit of output as a virtual tax, similar to a value-added tax. Taxes on consumption tend to have distortionary effects, because they change incentives for consumption, labour and saving. They lower demand and consequently lower aggregate production. This reduction in production is an extra cost to society, typically referred to as a *deadweight loss*.

In the case of consumption taxes, the deadweight loss is typically substantial in proportion to the tax revenue, and sometimes even exceeds it. However, since the deadweight loss does not refer to any observable number, they are more difficult to estimate or even understand. [43] explained that policy makers often ignore the distortionary effects of tax changes.

In assessing the economic impact of cyber crime we must avoid a similar negligence. The market distortions indirectly caused by cyber crime could conceivably form a substantial cost to economy in comparison to the immediate losses and expenses.

Cyber crime also creates market *frictions*: costs and inconveniences associated with the trade of goods and services. This mostly applies to online services like webshops and e-health portals, and includes for example the inconvenience of two-factor authentification. Disruptive attacks, like denial-of-service attacks, can also be seen as a market frictions, since they prevent trades from being executed smoothly.

By calling such matters market frictions we emphasise that their true costs consist of not just the immediate inconvenience, but also the resulting decrease in demand. For instance, consumers may forego purchases if an online store or payment system is temporarily offline after a cyber attack.

### Tax distortions

A similar argument can be made about the distortionary effect of government spending. Law enforcement, awareness campaigns and other initiatives undertaken by government are mostly financed by tax money. As explained before, any tax has distortionary effects on the behaviour of economic agents, in such matters as consumption and labour-leisure tradeoffs. This brings about a deadweight loss to society.

### Slowing down of innovation

Cyber security risks may deter business from investing in innovation. This may happen in one of two ways: (1) a business interested in developing or implementing a new IT solution may decide that the associated cyber security risks would render it inoperable or unprofitable, or (2) the risk of cyber-facilitated corporate espionage diminishes the competitive advantage that R&D might bring.

In a vacuum, theft of intellectual property or trade secrets is not necessarily bad for society. Exclusive access to IP allows its owner to charge monopoly prices, which is well known to be economically inefficient. Corporate espionage sets a level playing field and forces businesses to compete on price. This tradeoff between access and incentives for innovation is reflected in patent rights, for example, which protect IP owners but only for a limited period [107]. Corporate espionage may throw off this balance and reduce incentives for innovation.

This problem is not restricted to the private sector. In the healthcare sector, for instance, the government plays an important role in innovation, either as initiator or as lawmaker. In the Netherlands, the introduction of a nationwide electronic patient file system has been delayed by a heated political debate about security and privacy risks that continues to this day.

### Effects on competition

Cyber crime affects different businesses, sectors, and nations in different ways. This may skew competition. For example, one might say that cyber criminals mostly target large corporations for their valuable information assets, while smaller companies are left alone. Others might argue that cyber security investment displays economies-of-scale, which favours larger companies and creates entry barriers.

As we have established previously, cyber crime poses many different costs to organisations. The magnitude varies based on sector, organisation size, information assets, intensity of cyber attacks, and so on. This variability between firms may have important consequences for competition within and between sectors and nations.

Another way in which cyber crime may distort market competition is by making businesses more likely to move development of IT systems in-house, with the maxim that "you cannot outsource risk".

# How to estimate costs: measuring, modelling and calibrating

Many of the challenges that emerge when estimating the costs of cybercrime still remain unresolved. While some of these challenges are conceptual, the main issues are empirical. Conceptual issues have been discussed at length in the previous chapter. In this chapter, we focus on describing how to address empirical issues in order to generate cost estimates.

A myriad of empirical issues arise because estimating the costs of cybercrime requires vast amounts of information. Current data sources simply either do not capture the information necessary to create accurate estimates or is not available in suitable format (see Section 2). For instance, establishing how much time defence forces spend in fighting cybercrime becomes hardly possible as time inputs are distributed among many different types. There are countless other hurdles of a similar kind. Estimating the costs to victims of cyberattacks, for example, requires very large victim surveys to ensure adequate coverage of the range of attacks that might result from the rarer types of attacks (e.g. ransomware). But it is also very clear that the data collected from these surveys form only one side of the equation. The very reason why society invests resources on cybercrime prevention is to lower its impact both in economic and non-economics terms. Increasing thought is being given to the methodology for making estimates in settings where data are poor and to the transferability of estimates between sectors and countries [98]. However, currently no single data source is comprehensive enough to allow generating accurate estimates of cybercrime.

As a result of these challenges, it becomes a chimerical task to develop a single approach that robustly measures the costs of cybercrime. In the following, we describe the techniques to estimate the costs as described in our economic model.

## 4.1 Measuring costs in anticipation of cybercrime

Potential cybercrime victims are willing to take measures to reduce the risk and impact of victimisation. These measures include defensive strategies (e.g., air gaping) to precautionary behaviour (e.g., bring your own device (BYOD) policies) [79].

The main anticipation costs come from the expenditure on the acquisition of security products and services. Data on security measures have been collected across different countries and actors via surveys. For instance, the 2006-2007 ENISA "Survey on Security and Anti-Spam Measures of Electronic Communication Service Providers" provided information on security and anti-spam measures which were deployed by providers [81]. Regarding generic businesses, the CSI/FBI [30] surveys constitute another source of information covering US companies. These surveys analysed security technologies in place, such as Digital IDs, intrusion detection systems, physical security, firewalls, antivirus software, biometrics, etc. Additionally, the E&Y Global Information Security Survey reports on the costs of companies from 27 different sectors with threat intelligence programs and breach detection programs [37]. Many other surveys also covered direct costs associated with the deployment of security measures (see table A.1). As reported by the SANS institute, some companies prefer to outsource security which provides an estimate of the expenditure in security including anticipation (e.g. monitoring of infrastructure, monitoring of security controls, etc.) [114].

Besides the expenditure on security products and services, organisations and individual agents may also need to invest on IT infrastructure to reduce the impact of a potential cyber attack. For instance, replicating data servers or buying load balancers could be necessary infrastructure to mitigate the impact of DDoS attacks. Some data regarding IT investment as anticipation cost can be found in the Ponemon institute reports [104, 102] and the Global information security survey conducted by Ernst&Young [37].

Anticipation measures also impact the productivity of employees. Organisations need to develop tactics to detect and detract potential cyber attacks. Developing and implementing these tactics affect the productivity of employees that need to be aware of these tactics and be able to use adequately the security measures in place. However, the productivity loss due to the deployment of anticipation measure cannot be measured directly. Data on the time spent on security-related tasks can be used as proxy to estimate this type of cost. For instance, the Black Hast 2015 Attendee survey estimated which security activity consumed the greatest amount of time [128].

Moreover, anticipation strategies do not exclusively limit themselves to train employees

in the usage of the defence measures, but also make them aware of the existing cyber threats. As Johnson [72] pointed out, security awareness programmes have major costs such as (i) the salary of the security awareness coordinator or team; (ii) training, including teacher fees and room rentals; and (iii) materials, such as slides, posters, videos, handouts and gadgets. But these are not all the costs. Security awareness programmes also impact on the trainee's productivity. In this sense, the 2015 SANS Security Awareness Report measured the time spent on security awareness by both level and organisation size [116]. More specifically, the Ponemon report on 'The Cost of Phishing & Value of Employee Training' [105] estimated the financial impact of phishing on employee productivity and how training could reduce this impact. The series of CSI/FBI surveys also include estimates of the cost of awareness training as a percentage of the security budget [30].

Anticipation measures also include maintaining current deployed security measures (e.g. hardware and software). One critical part of this maintenance consists in patching known vulnerabilities. The costs associated with patch management strategies highly vary. For instance, every time Google patches the kernel on workstations of its employees, the subsequent reboot of the machines costs them $1 million in lost productivity [12]. All costs related to patch applications can be estimated by using system administrator time as proxy. The SANS institute 2015 report on the state of application security estimated the time that it takes for an organisation to patch vulnerabilities [115].

Costs associated with administering cyberinsurance are similar to those of administering traditional crime insurance. Though most of these costs are for claims and underwriting administration, there are a number of other related expense items which add costs for funds but are not quantifiable as they are generally not segregated from other expenses. These include consulting/legal/tax advice (around insurance), record establishment, record updating, reporting, communication/disclosure and compliance. However, no data was found in this sense regarding cyberinsurance. An estimate could be derived from traditional insurances where public reports are available [148]. Nevertheless, as pointed in Section 2 the market for cyberinsurance is still too small to give a representative view of many different types of events.

Other anticipation costs are due to the confidence decrease on online services, i.e., there are barriers that prevent the agents from deploying more activities online. For instance, the SANS report on the security spending in the financial sector [114] describes 4 different type of barriers, i.e., (i) fear of false positives blocking legitimate business; (ii) concerns about throughput of data parsing; (iii) issues with interoperability between our security device and the monitoring support structure; and (iv) existing network bandwidth

limitations. Each of these barriers propagates some costs that mostly are intangible and hard to estimate.

## 4.2 Measuring costs as a consequence of cyber crime

Cybercrimes impose many different kinds of losses on both victims and society. As indicated above, our assessment of the consequential costs of cybercrime follows the approach of estimating: (i) business disruption; (ii) insurance claims; (iii) reputation damage and costumer attrition after data breaches; and (iii) loss of competitive advantage due to IP theft.

Several surveys provide data on business disruption [102, 104, 124, 114, 105]. For instance, the 2014 survey conducted by the Ponemon institute [102] described that on an annualised basis, business disruption accounts for 38% of total external costs, which include costs associated with business process failures and lost employee productivity. However, business disruption can also be estimated by analysing security data. In the case of Distributed Denial of Service (DDoS) attacks, honeypots and data from security providers can provide insights on the amount of time a network was disrupted and use this as proxy to estimate the costs. Several cyber incident data sources exist and can be use to this purpose (see table A.3). For instance, Arbor Networks provides yearly reports on DDoS attack duration and intensity [14]. Some news reports also provide some figure on different costs due to business disruptions. Table A.5 serves as an example of news article reporting about the cost of cybercrime incidents. However, one should be extremely careful when using new reports data to generate estimates as they tend to be tremendously biased (see chapter 2).

The costs due to cyberinsurance claims illuminates the real costs of incidents from an insurer's perspective. There exist various costs associated with an cyberinsurance claim: crisis services (forensics, notification, credit/ID monitoring, legal counsel and miscellaneous other), legal damages (defence and settlement), regulatory action (defence and settlement) and PCI fines. NetDillengence has conducted several studies during the last years by interviewing insurance underwriters about data breaches and the claim losses they sustained [55]. Though these data is clearly biased due to victims' underreporting incentives, it gives an estimate of the cost of actual cyberinsurance claims. McAfee and PwC efforts to estimate the global cost of cybercrime also provide some insights of the costs of cyberinsurance claims [84, 10].

However, the reputation damage due to cybercrime is not directly measurable. Several

proxies can be used to estimate these costs. The International Cyber Security Protection Alliance (ICSPA) conducted a study to analyse the reputation damage as a result of cyber crime attacks [67]. This study used variables such as sabotage of data/networks or misuse of social networks as proxies to estimate this cost. The Ponemon Institute also conducted a survey to estimate what reputation and brand damage can cost as a result of the loss of customers [100].

Finally, the last cost as consequence of cybercrime is the loss of competitive advantage due to intellectual property or data theft. Numerous academic, industry, non-profit and government reports highlight the challenges in estimating the overall value of intellectual property and the economic impact of those that are stolen. When it comes to estimate the costs of IP theft, the most comprehensive study is the one conducted by Detica [34]. IP thefts also lead to material damages that are less tangible but no less adverse, including: loss of product/market advantage, missed business opportunity, loss of reputation or brand loyalty, declines in stock price or valuation, direct loss of profitability and lawsuits. PwC tried to capture these costs by using research and development investment as proxies [9]. They also used illicit economic activity (i.e. occupation fraud, tax evasion, corruption, black market activities and illicit financial flows) as proxy. On the other hand, several breach data repositories exist (see Table A.2). These repositories vary on size, sources and the type of records they keep. Some of these records are self-reported which skew the dataset. Among the most complete repositories DatalossDB [95], Privacy Rights Clearinghouse [51] (PRC), and Identity Theft Resource [63] provide useful data. DatalossDB keeps record of data breaches since 1995 and publishes a monthly report. PRC responds to specific privacy-related complaints from users, capturing the nature and details (Type of Breaches, Organisation Type(s), the Size of Breach, Date of Incidence, and verifiable Source of Report) of the complaints, questions and reports them to policy makers, the public, advocates and the media. Finally, it is worth mentioning the Vocabulary for Event Recording and Incident Sharing (VERIS) [144] model designed to provide a common language for describing security incidents in a structured and repeatable manner.

## 4.3 Measuring costs in response to cybercrime

Response to cybercrime comes mainly from the criminal justice system. The various types of response entail costs including the ones associated to police forces, prosecution, courts, legal fees, criminal sanctions, victim and witness costs, jury service, incarceration, criminal code review and over-deterrence costs. When these institutions are in modern states financed by public sources, data is readily available. However, even though most

of these costs are tangible and some of them could be estimated as in traditional crime, little data exist for cybercrime.

Most of the publicly available reports concerning the justice system expenditures do not differentiate between traditional crime and cybercrime. As Cohen Mark [28] pointed out even if accurate, aggregate criminal justice expenditures are of little value in estimating the economic impact of crime. As noted, police officers do more than enforce criminal laws; they also deal with traffic safety and other community issues. For example, the Bureau of Justice Statistics periodically estimates annual justice expenditures in the United States [52] but it is not specified what part of these expenditures are specific to cybercrime.

Exceptionally, some countries do report some data related to the impact of cybercrime on the criminal justice system (see table A.4). For example, the Spanish Ministry of Interior reports yearly the amount of convictions and offences related to cybercrime [121]. Similarly, the figures that UK Home Office ministers released on 2015 showed the average number of convictions under the Computer Misuse Act per month for the past 23 years [36]. Smith et al. [120] provided the first international study of the manner in which cyber criminals are dealt with by the judicial process. Nevertheless, as Smith et al. [120] states there is a considerable attrition in numbers of cybercrimes that are being perpetrated, the number that are reported to the police and other official agencies for investigation, and the number that result in judicial proceedings and (on occasions) punishment of offenders. Therefore, using the number of convictions as the societal response cost to cybercrime generates a lower bound of these costs.

Additional costs arise with cybercrime as compared to traditional crime when it comes to obtaining evidence. Obtaining electronic evidence can result very expensive, as forensic accountancy services may need to be used and large amounts of data examined. Smith et al. [120] also points out that in cross-border cases, the procedures for obtaining mutual legal assistance are also slow and some countries are not parties to international conventions. These costs are hard to calculate and currently no accurate data exist that allow estimating them.

Moreover, specialised institutions have been created to manage cyber incidents and cyber threats. These constitute additional costs. Computer Emergency Response Teams (CERTs) are the main example of these institutions. The costs of CERTs depend on their functions and capabilities. ENISA conducted a survey in order to asses different CERT (national/governmental and non-governmental) and estimate their funding model [39].

## 4.4 Estimating long term distortionary effects

In most cases we cannot directly measure or observe the economic distortions described in Section 3.5. Even if we can quantify certain economic inefficiencies, it is often not clear how much of this we can attribute to the existence of cyber crime.

Analysing the long term economic implications of cyber crime goes beyond simple measurements and estimations, and generally requires much stronger modelling assumptions. Hence, the usefulness and adequacy of existing data sources depends to a large extent on the used models and estimation methods.

In this section we briefly examine two opportunities for analysing the long term economic effects of cyber crime and the kind of data that might contribute to such analysis, but we emphasise that this is by no means intended as a comprehensive list of relevant data sources and estimation methods.

### Consumer avoidance

The effect of security concerns on the adoption and use of online services seems in principle to be measurable. For instance, a recent report based on a survey among 10,000 consumers in the U.S. and UK, found that "77% of international consumers report that they do not feel safe while transacting through the web" and that "23% of consumers said they were shopping less online during the holidays due to security concerns" [90].

There are however two methodological difficulties in determining the *economic cost* of this avoidance effect. First, it is not trivial to determine the economic efficiency created by these online channels. A greater (or faster) adoption of online banking could allow banks to close some of their branches, but maintaining an online payment infrastructure is costly as well. The long term economic benefits of adoption of online banking are even more difficult to assess. The same can be said about the economic benefits of online shopping.

The second challenge is to figure out what part of these economic inefficiencies we can attribute to cyber crime. A consumer's choice of whether to use online services is influenced by a great many factors besides her security concerns, and even the consumer herself may not realise exactly how such decisions are made. Hence, even if consumers state explicitly that security is the reason they do not shop or bank online, we cannot

attribute the full economic cost of their avoidance to cyber crime.

The second issue was previously addressed by project partners [110]. They created a variant of the Technology Acceptance Model that identifies several factors contributing to a consumer's decision of whether to use online services. In subsequent analysis in this work package we will build upon this work.

### Effects on competition

To study the variability in the costs of cyber crime to different organisations, sectors, and nations, we would ideally have fine-grained data at the level of individual organisations. Several reports based on organisation surveys presented some results at the sector level. For example, Ponemon Institute [102] compared security spending in different industries, based on their survey results. Comparisons of survey answers by organisation size are also common, although typically these are tersely reported.

For the most part, though, we have to rely on more qualitative assessments and theories. Such efforts can be helped by qualitative interviews and surveys among security professionals. To illustrate, Libicki et al. [79] created a mathematical model of the relation between organisational characteristics — like staff size and the number of connected devices — and the impact of cyber crime, based on insights gained from qualitative interviews with CISOs. They demonstrated with simulations of this model that the costs of cyber crime vary strongly between different organisational types. In particular, their simulation study suggested that organisations with large networks are intrinsically unable to protect the whole perimeter of their network, and must instead focus on limiting internal access to sensitive information to reduce the damage that intruders can do.

There are different data sources that may help us to calibrate such models. For instance, threat intelligence reports [e.g. 125] may give us an idea of how intensively businesses of different type and size are attacked.

# Conclusions

In this deliverable we have argued that estimating the costs of cybercrime is a valuable, and indeed irreplaceable, tool for policy makers and the criminal justice system. However, while the concept of monetizing the impact of cybercrime, for many people seems feasible, and maybe even reasonable, such calculations have many disadvantages and generate estimates that are from reality.

From the analysis based on the state-of-the-art we have identified the drawbacks of current cybercrime studies and described the challenges that have to be addressed before generating cost estimates. Moreover, we have analyzed existing data sources depending on the measurement methodology and how different aggregation models have leveraged these data to generate unrealistic costs estimates. Due to the misuse and limitations of existing data sources, the true burden of cybercrime on human society still remains unknown.

To fulfill this information gap, we have derived a set of basic economic foundations that serve as basis for our model. First, we have defined what a cost is. Once clarified, we have divided the cost of cybercrime into different levels: cost of cybercrime to individual agents and cost of cybercrime to society. Costs of cybercrime to individual agents are costs which are direct consequences of crime and can be classified into three different categories, namely, anticipation, consequence and response costs. Lastly, we have also investigated the societal impact of cybercrime and assessed the adequacy of existing data sources for our economic model.

In the next period two tasks will be carried out: the first one will be focused on the calibration of our model on the selected non-ICT sectors with the data collected during the consumer survey and the industry interviews. Additional external data sources will

be used to calibrate some parts of the model that are not captured by the data gathered during previous workpackages. Finally, we will use the material produced in the previous task and validate the results and model with a group of stakeholders different from those involved in the interviews.

# Appendices

# Appendix A: Mapping sources to economic model

| | | Anticipation | | | | | | | | Consequence | | | | | Response | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization | Title | Security controls | Insurance admin | Awareness campaigns | IT Infra. Investment | Productivity loss | Lower confidence online | Security due diligence | Patch development | Business disruption | Reputation damage | Pain and suffering | Insurance claims | Loss competitive adv. | Criminal Justice System | CERTs and CSIRTs |
| CSI/FBI | Computer Crime and Security Survey [30] | ■ | | ■ | | | | | | ■ | | ■ | | | | |
| Detica | The cost of cyber crime [34] | | | | | | | | | | ■ | | | ■ | | |
| Ponemon | Cost of Cyber Crime [102] | ■ | | | ■ | ■ | | | | ■ | | | | | | |
| FSB | Cyber security and fraud: The impact on small businesses [42] | ■ | | ■ | | | | | ■ | | | | | | | |
| Symantec | Norton Cybercrime Report [124] | | | | | | | | | ■ | ■ | | | | | |
| McAfee | Net Losses: Estimating the Global Cost of Cybercrime [84] | ■ | | | | | ■ | | | | ■ | | ■ | ■ | | |
| Deloitte | Irish Information Security and Cybercrime Survey [33] | ■ | | | | | | | | | ■ | | | | | |
| PwC | Global Economic Crime Survey [10] | ■ | | | | | | | | ■ | ■ | | ■ | | | |
| SANS | State of Application Security [115] | ■ | | ■ | | | | | ■ | | | | | | | |
| SANS | Security Awareness Report [116] | | | ■ | | | | | | | | | | | | |
| SANS | Security Spending and Preparedness in the Financial Sector [114] | ■ | | | ■ | | ■ | | ■ | ■ | ■ | | | | | |
| Ponemon | Cost of Phishing & Value of Employee Training [105] | ■ | | ■ | | ■ | | | | ■ | | | | | | |
| Blackhat | Black Hat Attendee Survey [128] | ■ | | ■ | | ■ | | | | | | | | | | |
| Symantec | Endpoint Security Best Practices Survey [31] | | | | | | | | | ■ | ■ | ■ | | | | |
| Ponemon | State of the Endpoint Report [104] | ■ | | | ■ | | | | | | | | | | | |
| Ernst&Young | Global information security survey [37] | ■ | | ■ | ■ | | | | ■ | | | | | | | |

Table A.1: Map of existing surveys to our economic model

| | | Anticipation | | | | | | | | Consequence | | | | | Response | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization | Title | Security controls | Insurance admin | Awareness campaigns | IT Infra. Investment | Productivity loss | Lower confidence online | Security due diligence | Patch development | Business disruption | Reputation damage | Pain and suffering | Insurance claims | Loss competitive adv. | Criminal Justice System | CERTs and CSIRTs |
| Safenet | Breach Level Index [113] | | | | | | | | | ■ | ■ | | | ■ | | |
| PRC | Privacy Rights Clearinghouse [51] | | | | | | | | | ■ | ■ | | | ■ | | |
| Open Security Foundation | DataLossDB [95] | | | | | | | | | ■ | ■ | | | ■ | | |
| IRTC | ITRC Breach Database [63] | | | | | | | | | ■ | ■ | | | ■ | | |
| Verizon | The VERIS Community Database (VCDB) [144] | | | | | | | | | ■ | ■ | | | ■ | | |
| DataBreaches.net | DataBreaches.net [2] | | | | | | | | | ■ | ■ | | | ■ | | |
| PwC | Information security breaches survey 2015 [108] | ■ | | ■ | ■ | | | | | ■ | ■ | | | ■ | | |
| Ponemon/IBM | Cost of Data Breach Study [140] | | | | | | | | | ■ | ■ | | | | | |
| Verizon | 2014 Data Breach Investigations report [103] | ■ | | | | | | | | ■ | | | | ■ | | |
| Ponemon | 2014 Survey on Medical Identity Theft [101] | | | | | | | | | ■ | ■ | | | | | |

Table A.2: Map of existing data breach repositories and studies to our economic model

| | Anticipation | | | | | | | | Consequence | | | | | Response | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Title | Security controls | Insurance admin | Awareness campaigns | IT Infra. Investment | Productivity loss | Lower confidence online | Security due diligence | Patch development | Business disruption | Reputation damage | Pain and suffering | Insurance claims | Loss competitive adv. | Criminal Justice System | CERTs and CSIRTs |
| DNS-BH Malware Domain Blocklist [131] | | | | | | | | | ■ | | | | | | |
| MalwareURL [4] | | | | | | | | | ■ | | | | | | |
| Dshield [69] | | | | | | | | | ■ | | | | | | |
| Google Safe Browsing Alerts [54] | | | | | | | | | ■ | | | | | | |
| HoneySpider Network [146] | | | | | | | | | ■ | | | | | | |
| FIRE (FInding Rogue nEtworks) [145] | | | | | | | | | ■ | | | | | | |
| Team Cymru – TC Console [126] | | | | | | | | | ■ | | | | | | |
| Zeus/SpyEye Tracker [11] | | | | | | | | | ■ | | | | | | |
| Malware Domain List [6] | | | | | | | | | ■ | | | | | | |
| The Spamhaus Project [131] | | | | | | | | | ■ | | | | | | |
| Shadowserver Foundation [7] | | | | | | | | | ■ | | | | | | |
| SGNET / Leurre.com Honeynet Project [147] | | | | | | | | | ■ | | | | | | |
| Malc0de database [3] | | | | | | | | | ■ | | | | | | |
| ParetoLogic URL Clearing House [97] | | | | | | | | | ■ | | | | | | |
| SpamCop [25] | | | | | | | | | ■ | | | | | | |
| Arbor ATLAS [15] | | | | | | | | | ■ | | | | | | |
| Composite Blocking List [130] | | | | | | | | | ■ | | | | | | |
| Team Cymru's CSIRT Assistance Program [127] | | | | | | | | | ■ | | | | | | |
| Project Honeypot [137] | | | | | | | | | ■ | | | | | | |
| Smart Network Data Services [5] | | | | | | | | | ■ | | | | | | |
| Malware Patrol [5] | | | | | | | | | ■ | | | | | | |
| Zone-H [8] | | | | | | | | | ■ | | | | | | |
| SenderBase [26] | | | | | | | | | ■ | | | | | | |
| Anti-Phishing Working Group [56] | | | | | | | | | ■ | | | | | | |

Table A.3: Map of existing incident data to our economic model

| | | Anticipation | | | | | | | | Consequence | | | | | Response | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization | Title | Security controls | Insurance admin | Awareness campaigns | IT Infra. Investment | Productivity loss | Lower confidence online | Security due diligence | Patch development | Business disruption | Reputation damage | Pain and suffering | Insurance claims | Loss competitive adv. | Criminal Justice System | CERTs and CSIRTs |
| AusCERT | Cyber crime & security survey report [16] | ■ | | ■ | ■ | | | | | | | | | | | |
| Brazilian CERT | Distributed Honeypot Project [20] | | | | | | | | | ■ | | | | | | |
| Polish CERT | ARAKIS [99] | | | | | | | | | ■ | | | | | | |
| Brazilian CERT | Spampots [21] | | | | | | | | | ■ | | | | | | |
| ENISA | Provider Security Measures [81] | ■ | | | | | | | | | | | | | | |
| IC3 | Internet Crime Complaint Center Annual Reports [40] | | | | | | | | | ■ | ■ | | | ■ | | |
| INCIBE | Information Security and e-Trust in Spanish households [65] | ■ | | | | | ■ | | | ■ | | | | | | |
| NSCS | Cyber Security Assessment Netherlands [91] | ■ | | | | | | | | ■ | | | | ■ | | |
| Japanese IT Security Centre | Major Security Threats [70] | ■ | | | | | | | | | | | | | | |
| OECD | Measurement of trust in the online environment [96] | ■ | | | | | ■ | | | | | | | | | |
| BSI | IT Security Situation in Germany [41] | ■ | | | | | | | | | | | | | | |
| SIBIS | Benchmarking Security and Trust [109] | | | | | | ■ | | | | | | | ■ | | |
| Belgian CERT | Reported incidents [17] | | | | | | | | | ■ | | | | | | |
| Estonian CERT | Annual Report Cyber Security [38] | ■ | | ■ | | | | | | ■ | | | | | | |
| Finish CERT | Cyber Security Review [44] | ■ | | ■ | | | | | | ■ | | | | | | |
| French CERT | Bulletins d'actualité [47] | | | | | | | | | ■ | | | | | | |
| Icelandic CERT | Annual incidents report [62] | | | | | | | | | ■ | | | | | | |
| Swiss CERT | Information Security in Swiss Companies [123] | ■ | ■ | ■ | | | | | | ■ | | | | | | |

Table A.4: Map of existing governmental reports to our economic model

| | | Anticipation | | | | | | | | Consequence | | | | | Response | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization | Title | Security controls | Insurance admin | Awareness campaigns | IT Infra. Investment | Productivity loss | Lower confidence online | Security due diligence | Patch development | Business disruption | Reputation damage | Pain and suffering | Insurance claims | Loss competitive adv. | Criminal Justice System | CERTs and CSIRTs |
| TechRepublic | Calculating the true cost of cybercrime [118] | ■ | | | | ■ | | | | ■ | | ■ | | ■ | | |
| Engineering and Technology Magazine | News analysis: Calculating the true cost of cybercrime [18] | | ■ | | | | | | | | ■ | | | ■ | | |
| ProPublica | Does cybercrime really cost $1 Trillion? [80] | | | | | ■ | | | | ■ | | | | | | |
| The Economist | WhatâĂŹs in a number? Estimating the true cost of cybercrime [129] | ■ | | | | | | | | ■ | | | | | | |
| ComputerWorld | $445 billion: Bloated BS or the true cost of cybercrime [122] | | | | | | | | | ■ | | | | | | |
| FSE Group | Cost-effective ways to shield SMEs from cybercrime [48] | | | | | | | | | | ■ | | | | | |
| The Telegraph | Cost of online dating scams jumped 16pc last year, say police [133] | | | | | | ■ | | | | | ■ | | | | |
| Daily Mail | How police 'ignore cybercrime' [134] | | | | | | | | | | | | | | ■ | |
| The Mirror | One computer hacker a month convicted of cyber crime out of 100,000 incidents a year [36] | | | | | | | | | | | | | | ■ | |

Table A.5: Map of cybercrime-related news to our economic model

# References


[1] The Honeynet Project. https://www.honeynet.org/papers, 2015.

[2] Databreaches.net. http://www.databreaches.net/, 2015.

[3] Malc0de database. http://malc0de.com/database/, 2015.

[4] MalwareURL. http://www.malwareurl.com, 2015.

[5] Malware Patrol. http://www.malwarepatrol.net, 2015.

[6] Malware Domain List. http://www.malwaredomainlist.com/, 2015.

[7] The Shadowserver Foundation. http://shadowserver.org/, 2015.

[8] Zone-H. https://www.zone-h.org/, 2015.

[9] PricewaterhouseCoopers (PwC). Economic Impact of Trade Secret Theft. https://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf, 2014.

[10] PricewaterhouseCoopers (PwC). Global State of Information Security survey. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey, 2015.

[11] Abuse.ch. Zeus/SpyEye/Feodo Tracker. https://abuse.ch, 2015.

[12] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy*, pages 265–300. Springer Berlin Heidelberg, 2013.

[13] D Anselmi, J Kuo, R Boscovich, et al. Microsoft security intelligence report, 2010.

[14] D Anstee, A Cockburn, and G Sockrider. Worldwide infrastructure security report. Technical report, Technical report, Burlington, MA, USA, 2014.

[15] Arbor Networks. Active Threat Level Analysis System. http://atlas.arbor.net/, 2015.

[16] Australia, CERT. Cyber crime & security survey report 2013. https://www.cert.gov.au/system/files/614/679/2013%20CERT%20Australia%20Cyber%20Crime%20%2526%20Security%20Survey%20Report.pdf, 2013.

[17] Belgian CERT. Figures about incidents reported to CERT.be. https://www.cert.be/files/CERTbe_Statsoverview2010-2014-EN.pdf, 2014.

[18] Hugh Boyer. News analysis: Calculating the true cost of cybercrime. http://eandt.theiet.org/magazine/2013/08/news-analysis-cybercrime.cfm, 2013.

[19] Sam Brand and Richard Price. *The economic and social costs of crime*. Home Office London, 2000.

[20] Brazilian CERT. Distributed Honeypot Project. http://honeytarg.cert.br/honeypots/, 2015.

[21] Brazilian CERT. SpamPots Project. http://honeytarg.cert.br/spampots/, 2015.

[22] Matthias Brecht and Thomas Nowey. A closer look at information security costs. In *The Economics of Information Security and Privacy*, pages 3–24, 2013. ISBN 978-3-642-39497-3.

[23] Katherine Campbell, Lawrence A Gordon, Martin P Loeb, and Lei Zhou. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448, 2003.

[24] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1):70–104, 2004.

[25] Cisco Systems. SpamCop. https://www.spamcop.net/, 2015.

[26] Cisco Sytems. IronPort SenderBase Security Network. http://www.senderbase.org/, 2015.

[27] M.A. Cohen. *The Costs of Crime and Justice*. Taylor & Francis, 2004. ISBN 9781135994501.

[28] A Cohen Mark. Measuring the costs and benefits of crime and justice. *Measurement and Analysis of Crime and Justice. Criminal Justice 2000*, pages 263–315, 2000.

[29] Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI). Computer Crime and Security Survey. htpp://www.gocsi.com, 1996.

[30] Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI). Computer Crime and Security Survey. http://gatton.uky.edu/FACULTY/PAYNE/ACC324/CSISurvey2011.pdf, 2011.

[31] Symantec Corporation. 2012 Endpoint Security Best Practices Survey. https://www.symantec.com/content/en/us/enterprise/white_papers/b-2012_endpt_sec_best_practices_survey_results_WP.en-us.pdf, 2012.

[32] Jacek Czabanski. *Estimates of cost of crime: history, methodologies, and implications*. Springer Science & Business Media, 2008.

[33] Deloitte. Irish information security and cybercrime survey. http://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/cybercrime_survey_risk_2013_deloitte_ireland.pdf, 2013.

[34] Detica and Office, Cabinet. The Cost of Cybercrime: A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf, 2011.

[35] Goldthwaite Higginson Dorr, Sidney Post Simpson, and United States Wickersham Commission. *Report on the Cbst of Crime and Criminal Justice in the United States*. Washington, U.S. Govt. Print. Off., 1931.

[36] Matthew Drake. One computer hacker a month convicted of cyber crime out of 100,000 incidents a year. http://www.mirror.co.uk/news/uk-news/one-computer-hacker-month-convicted-5461766, 2015.

[37] Young LLP Ernst and XII Young. Global information security survey. *UK: Presentation Services*, 2014.

[38] Estonian CERT. 2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority. https://www.ria.ee/public/Kuberturvalisus/RIA-Kyberturbe-aruanne-2014_ENG.pdf, 2014.

[39] European Network and Information Security Agency (ENISA). Baseline capabilities of national/governmental certs. https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012, 2012.

[40] FBI. Internet Crime Complaint Center Annual Reports. https://www.fbi.gov/news/news_blog/2014-ic3-annual-report, 2014.

[41] Federal Office of Information Security. IT Security Situation in German. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf, 2014.

[42] Federation of small businesses. Cyber security and fraud: The impact on small businesses. http://www.fsb.org.uk/policy/assets/fsb_cyber_security_and_fraud_paper_final.pdf, 2013.

[43] Martin S. Feldstein. Effects of Taxes on Economic Behavior. Working Paper 13745, National Bureau of Economic Research, January 2008. URL http://www.nber.org/papers/w13745.

[44] Finish CERT. Cyber Security Review. https://www.viestintavirasto.fi/attachments/tietoturva/EN_osavuosikatsaus_II_2014.pdf, 2014.

[45] Kristin M Finklea and Catherine A Theohary. Cybercrime: conceptual issues for congress and us law enforcement. Congressional Research Service, Library of Congress, 2012.

[46] Dinei A. F. Florêncio and Cormac Herley. Sex, lies and cyber-crime survey. In *The Economics of Information Security and Privacy*, 2011.

[47] French CERT. Bulletins d'actualité. http://cert.ssi.gouv.fr/site/index_act.html, 2015.

[48] FSE Group. Cost-effective ways to shield SMEs from cybercrime. http://www.growthbusiness.co.uk/growing-a-business/technology-for-business/2495371/costeffective-ways-to-shield-smes-from-cybercrime.thtml, 2015.

[49] Anindya Ghose and Bin Gu. Search Costs, Demand Structure and Long Tail in Electronic Markets: Theory and Evidence. SSRN Scholarly Paper ID 941200, Social Science Research Network, Rochester, NY, October 2006. URL http://papers.ssrn.com/abstract=941200.

[50] B Givens. Chronology of data breaches-privacy rights clearinghouse. https://www.privacyrights.org/data-breach, 2014.

[51] Beth Givens and Privacy Rights Clearinghouse. *Privacy Rights Clearinghouse*. Privacy Rights Clearinghouse, 1996.

[52] Lauren E Glaze and Thomas P Bonczar. Bureau of justice statistics. *population*, 1, 2007.

[53] Google. Google Transparency Report. http://www.google.com/transparencyreport/safebrowsing/, 2015.

[54] Google. Google Safe Browsing Alerts. http://safebrowsingalerts.googlelabs.com, 2015.

[55] Mark Greisiger. Cyber liability & data breach insurance claims a study of actual claim payouts. Technical report, NetDiligence, Tech. Rep, 2013.

[56] Anti-Phishing Working Group et al. Apwg phishing trends reports. http://www.antiphishing.org/phishReportsArchive.html, 20015.

[57] Eric R Hawkins and Willard Waller. Critical notes on the cost of crime. *Journal of Criminal Law and Criminology (1931-1951)*, pages 679–694, 1936.

[58] Cormac Herley and Dinei Florêncio. A Profitless Endeavor: Phishing As Tragedy of the Commons. In *Proceedings of the 2008 Workshop on New Security Paradigms*, NSPW '08, pages 59–70, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-341-9. doi: 10.1145/1595676.1595686. URL http://doi.acm.org/10.1145/1595676.1595686.

[59] Home Office and Office for National Statistics. UK Crime Survery. http://www.crimesurvey.co.uk/, 2014.

[60] Annelies Huygen, Natali Helberger, Joost Poort, Paul Rutten, and Nico Van Eijk. Ups and downs; economic and cultural effects of file sharing on music, film and games. *TNO Information and Communication Technology Series*, 2009.

[61] Paul Hyman. Cybercrime: It's Serious, but Exactly How Serious? *Commun. ACM*, 56(3):18–20, 2013. ISSN 0001-0782.

[62] Icelandic CERT. Annual incidents report. https://www.cert.is/files/CERT-IS.arsskyrsla2014.pdf, 2014.

[63] Identity Theft Research Center (IRTC). 2015 ITRC Breach Database. http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf, 2015.

[64] Imperva. The Top 10 DDoS Attack Trends. https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf, 2015.

[65] INCIBE. Study on Information Security and e-Trust in Spanish households. http://www.ontsi.red.es/ontsi/sites/default/files/ciberseguridad_y_confizanza_en_los_hogares_espanoles_feb_2015.pdf, 2014.

[66] Daisuke Inoue, Mio Suzuki, Masashi Eto, Katsunari Yoshioka, and Koji Nakao. Daedalus: Novel application of large-scale darknet monitoring for practical protection of live networks. In Engin Kirda, Somesh Jha, and Davide Balzarotti, editors, *Recent Advances in Intrusion Detection*, volume 5758 of *Lecture Notes in Computer Science*, pages 381–382. Springer Berlin Heidelberg, 2009. ISBN 978-3-642-04341-3.

[67] International Cyber Security Protection Alliance (ICSPA). Study of the impact of cyber crime on businesses in canada. https://www.icspa.org/wp-content/uploads/2014/12/ICSPA-Canada-Cyber-Crime-Study-Report.pdf, 2014.

[68] Internet Crime Complaint Center. 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_IC3report.pdf, 2010.

[69] Internet Storm Center. Dshield. http://www.dshield.org, 2015.

[70] Japanese IT Security Centre. Major Security Threats. https://www.ipa.go.jp/files/000016942.pdf, 2014.

[71] Jill Joerling. Data breach notification laws: An argument for a comprehensive federal law to protect consumer data. *Wash. UJL & Pol'y*, 32:467, 2010.

[72] Everett C. Johnson. Security awareness: switch to a better programme. *Network Security*, 2006(2):15 – 18, 2006. ISSN 1353-4858.

[73] K Kannan, Jackie Rees, and EH Spafford. Unsecured economies: Protecting vital information. *Red Consultancy for McAfee, Inc*, 2009.

[74] Kaspersky Lab. Global IT Security Risks Survey. http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf, 2015.

[75] Orin S Kerr. Cybercrime's scope: Interpreting 'access' and 'authorization' in computer misuse statutes. *NYU Law Review*, 78(5):1596–1668, 2003.

[76] Chris Kershaw, Sian Nicholas, and Alison Walker. *Crime in England and Wales 2007/08: Findings from the British Crime Survey and police recorded crime*. Home Office London, 2008.

[77] KPMG. Cybercrime survey report. https://www.kpmg.com/IN/en/IssuesAndInsights/ArticlesPublications/Documents/KPMG_Cyber_Crime_survey_report_2014.pdf, 2014.

[78] Monica Lagazio, Nazneen Sherif, and Mike Cushman. A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, 45:58 – 74, 2014. ISSN 0167-4048.

[79] Martin C Libicki, Lillian Ablon, and Tim Webb. *The DefenderâĂŹs Dilemma: Charting a Course Toward Cybersecurity*. Rand Corporation, 2015.

[80] Peter Maass and Megha Rajagopalan. Does Cybercrime Really Cost $1 Trillion? http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion, 2012.

[81] Pascal Manzano and Christian Rossow. Provider Security Measures: Survey on Security and Anti-Spam Measures of Electronic Communication Service Providers. Technical report, 2007.

[82] Dave Marcus and Ryan Sherstobitoff. Dissecting Operation High Roller. Technical report, McAfee, 2012.

[83] Michael G Maxfield. The national incident-based reporting system: Research and policy applications. *Journal of Quantitative Criminology*, 15(2):119–149, 1999.

[84] McAfee. Net losses: estimating the global cost of cybercrime: Economic impact of cybercrime II. http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf, 2014.

[85] McAfee and SAIC. Intellectual capital and sensitive corporate data now the latest cybercrime currency, 2011.

[86] Mike McGuire and Samantha Dowling. Cyber crime: A review of the evidence. 2013.

[87] Leigh B. Metcalf and Jonathan Spring. Blacklist Ecosystem Analysis Update: 2014. Technical report, Software Engineering Institute, 2012.

[88] Microsoft Research. A Profitless Endeavor: Phishing as Tragedy of the Commons. http://research.microsoft.com/apps/pubs/default.aspx?id=74159, 2008.

[89] Amalia R Miller and Catherine Tucker. Encryption and data loss. In *WEIS*, 2010.

[90] NCC Group. Trust in the Internet Survey. Technical report, NCC Group, 2014. URL https://whodoyou.trust/globalassets/documents/trust-in-the-internet-survey-paper.pdf.

[91] NCSC: Nationaal Cyber Security Centrum. Cyber Security Assessment Netherlands. https://english.nctv.nl/Images/cybersecurityassessmentnetherlands2014_tcm92-580598.pdf?cp=92&cs=65035, 2014.

[92] Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO). TNO: Cybercrime kost Nederland miljarden per jaar. http://www.automatiseringgids.nl/nieuws/2012/15/tno-cybercrime-kost-nederland-miljarden, 2012.

[93] NetDiligence. Cyber claims study 2014. http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf, 2014.

[94] BFH Nieuwesteeg. The legal position and societal effects of security breach notification laws, 2013.

[95] Open Security Foundation. Datalossdb. http://datalossdb.org/, 2015.

[96] Sam Paltridge, Sheridan Roberts, and B Beuzekom. Scoping study for the measurement of trust in the online environment. www.oecd.org/sti/35792806.pdf, 2005.

[97] ParetoLogic Inc. URL Clearing House. http://malwareblacklist.com/, 2015.

[98] A.R. Piquero and D. Weisburd. *Handbook of Quantitative Criminology*. Springer, 2010. ISBN 9780387776507.

[99] Polish CERT. ARAKIS Project. http://www.arakis.pl/pl/, 2015.

[100] Ponemon Institute. The 2013 eCommerce Cyber Crime Report: Safeguarding Brand And Revenue This Holiday Season . http://www.emc.com/collateral/analyst-reports/h12493-ar-2013-ecommerce-cyber-crime-report.pdf, 2013.

[101] Ponemon Institute. 2014 Survey on Medical Identity Theft. http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf, 2014.

[102] Ponemon Institute. 2014 Global Report on the Cost of Cyber Crime. http://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime, 2014.

[103] Ponemon Institute. Cost of Data Breach Study. http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF, 2015.

[104] Ponemon Institute. 2015 State of the Endpoint Report: User-Centric Risk. http://www.ponemon.org/local/upload/file/2015%20State%20of%20Endpoint%20Risk%20FINAL.pdf, 2015.

[105] Ponemon Institute. The Cost of Phishing & Value of Employee Training. http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf, 2015.

[106] Ponemon Institute. 2015 Cost of Cyber Crime Study: Global. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/, 2015.

[107] Richard Posner. Intellectual Property: The Law-and-Economics Approach. *Journal of Economic Perspectives*, page 57, January 2005. URL http://chicagounbound.uchicago.edu/journal_articles/310.

[108] Chris Potter and Andrew Beard. Information security breaches survey 2015. *Price Water House Coopers. Earl's Court, London*, 2015.

[109] RAND Europe. Benchmarking security and trust in europe and the us. *Statistical Indicators Benchmarking the Information Society (SIBIS)*, 22, 2003.

[110] M. Riek, R. Bohme, and T. Moore. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, PP(99):1–1, 2015. ISSN 1545-5971. doi: 10.1109/TDSC.2015.2410795.

[111] Edward M Roche. Internet and computer related crime: Economic and other harms to organizational entities. *Miss. LJ*, 76:639, 2006.

[112] Julie J. C. H. Ryan, D. Sc, and The George. The Use, Misuse, and Abuse of Statistics in Information Security Research, Presented to American Society of Engineering. In *Management National Conference (ASEM 2003)*, 2003.

[113] SafeNet/Gemalto. Breach level index. http://breachlevelindex.com, 2015.

[114] SANS Institute. Security Spending and Preparedness in the Financial Sector: A SANS Survey. https://www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032, 2015.

[115] SANS Institute. 2015 State of Application Security: Closing the Gap. https://www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942, 2015.

[116] SANS Securing The Human. 2015 Security Awareness Report. http://www.securingthehuman.org/media/resources/STH-SecurityAwarenessReport-2015.pdf, 2015.

[117] California Senate. California sb 1386 - personal information: Privacy. http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html, 2003.

[118] Deb Shinder. Calculating the true cost of cybercrime. http://www.techrepublic.com/blog/it-security/calculating-the-true-cost-of-cybercrime/, 2010.

[119] Sid Deshpande and Ruggero Contu. Market Share Analysis: Security Software, Worldwide, 2015.

[120] R.G. Smith, P. Grabosky, and G. Urbas. *Cyber Criminals on Trial*. Cambridge University Press, 2004. ISBN 9781139454810.

[121] Spanish Ministry of Interior. Statistical yearbook of the ministry of interior. http://www.interior.gob.es/documents/642317/1204854/Anuario_Estadistico_2013.pdf/b7606306-4713-4909-a6e4-0f62daf29b5c, 2013.

[122] Darlene Storm. $445 billion: Bloated BS or the true cost of cybercrime? http://www.computerworld.com/article/2476398/cybercrime-hacking/-445-billion--bloated-bs-or-the-true-cost-of-cybercrime-.html, 2014.

[123] Swiss CERT. A survey on threats, risk management and forms of joint action. https://www.melani.admin.ch/dam/melani/en/dokumente/informationssicherheit-studiedeutsch.pdf.download.pdf/study_informationsecurityenglish.pdf, 2014.

[124] Symantec Corporation. 2013 Cost of Data Breach Study: Global Analysis. http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-global-report-2013.en-us.pdf, 2013.

[125] Symantec Corporation. Internet Security Threat Report. https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347931_GA-internet-security-threat-report-volume-20-2015-appendices.pdf, 2015.

[126] Team Cymru. TC Console. https://www.tcconsole.com, 2015.

[127] Team Cymru. CSIRT Assistance Program. http://www.team-cymru.org/Services/CAP/, 2015.

[128] BlackHat/UBM Tech. 2015 Black Hat Attendee Survey. https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf, 2015.

[129] The Economist: Intelligence Unit. What's in a number? estimating the cost of cybercrime. http://www.economistinsights.com/technology-innovation/analysis/measuring-cost-cybercrime/, 2013.

[130] The SpamHaus Project. Composite Blocking List. http://cbl.abuseat.org/, 2015.

[131] The SpamHaus Project. DNSBL Datafeed. http://www.spamhaus.org/, 2015.

[132] The SpamHaus Project. Spam Trap Flow Statistics. http://www.abuseat.org/totalflow.html, 2015.

[133] The Telegraph. Cost of online dating scams jumped 16pc last year, say police. http://www.telegraph.co.uk/news/uknews/crime/11960852/Cost-of-online-dating-scams-jumped-16pc-last-year-say-police.html, 2015.

[134] The Telegraph. How police 'ignore cybercrime': Just one in 100 cases is investigated despite the number of online fraud cases rocketing in recent years. http://www.dailymail.co.uk/news/article-3247176/How-police-ignore-cybercrime-Just-one-100-cases-investigated-despite-number-online-fraud-cases-rocketing-recent-years.html, 2015.

[135] Trend Micro. Going Deeper: Exploring the Deep Web. http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploring-the-deep-web, 2015.

[136] Trend Micro. Open Global Spam Map. http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/index.html, 2015.

[137] Unspam Technologies. Project Honeypot. http://www.projecthoneypot.org, 2015.

[138] Michel van Eeten, Johannes Bauer, and Shirin Tabatabaie. Damages from internet security incidents. A framework and toolkit for assessing the economic costs of security breaches. 2009.

[139] Verisign. Distributed Denial of Service trends report. https://www.verisign.com/assets/report-ddos-trends-Q12015_en_IN.pdf, 2015.

[140] Verizon. 2015 data breach investigations report. https://its.ny.gov/sites/default/files/documents/rp_data-breach-investigation-report-2015_en_xg.pdf, 2015.

[141] Martin Wasik. The law commission's working paper on computer misuse. *Computer Law & Security Review*, 4(5):2 – 4, 1989. ISSN 0267-3649.

[142] Martin Wasik. The computer misuse act 1990. *Criminal Law Review*, pages 767–779, 1990.

[143] Martin Wasik. *Crime and the Computer*. Clarendon Press Oxford, 1991.

[144] S Widup. The veris community database. http://veriscommunity.net/, 2013.

[145] WOMBAT project. FIRE (FInding Rogue nEtworks). http://www.maliciousnetworks.org, 2015.

[146] WOMBAT project. HoneySpider Network. http://www.honeyspider.net, 2015.

[147] WOMBAT Project. SGNET 23 / Leurre.com Honeynet. http://www.wombat-project.eu, 2015.

[148] World Health Organization and others. Administrative costs of health insurance schemes: Exploring the reasons for their variability. 2010.