Beyond the pretty penny: the Economic Impact of Cybercrime

Carlos H. Gañán
Delft University of Technology
Jaffalaan 5, 2628 BX Delft
Delft 2628BX, The Netherlands
c.hernandezganan@tudelft.nl

Michael Ciere
Delft University of Technology
Jaffalaan 5, 2628 BX Delft
Delft 2628BX, The Netherlands
m.ciere@tudelft.nl

Michel van Eeten
Delft University of Technology
Jaffalaan 5, 2628 BX Delft
Delft 2628BX, The Netherlands
m.j.g.vaneeten@tudelft.nl

ABSTRACT

Over the past decade, considerable research effort has been devoted to articulating and measuring the various ways through which cyber crime impacts overall society. The large volume of literature on the topic contains few attempts to produce estimates of the financial impact of specific cyber incidents and little agreement on how to derive such estimates. An important substrata of this literature focuses on placing a monetary value on the costs of cyber crime but little is known about the long-term economic impact to society. In this article, we first assess the shortcomings of existing cost estimates and focus on the relevant issues pertinent to the feasibility of deriving valid and useful estimates beyond cost-benefit analyses. Following a mixed top-down/bottom-up methodology, we propose a theoretical framework to systematically identify the short and long-term impacts of cyber crime both at the agent and societal level. This framework serves as the foundation to assess the economic consequences of cyber crime beyond monetary costs.

ACM Reference format:
Carlos H. Gañán, Michael Ciere, and Michel van Eeten. 2017. Beyond the pretty penny: the Economic Impact of Cybercrime. In *Proceedings of New Security Paradigms Workshop, Islamorada, Florida, USA, October 2017 (NSPW'17),* 11 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Understanding the economic impact of cyber crime has never been as critical as it is today. Criminal statistics, industry and individual victim surveys show that cyber crime is on the rise, while the rates for other types of crime are decreasing. However, the assessment of the economic impact of cyber crime is incomplete and weak. Other than cyber security vendor data and third party surveys, we depend on victims identifying and communicating their experience of a cyber crime and their understanding of the attack vectors. Companies are reluctant to disclose information about cyber incidents they have suffered.

In this context, assessing the cost of cyber crime has been turned out to be a controversial undertaking. Everyone is familiar with the attention-grabbing estimates that put the cost of cyber crime 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 cyber crime" [18] — 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 cyber crime in a monetary amount. Such an amount is very parsimonious, we are familiar with thinking in terms of money and it seems to nicely fit the problem. We are talking about cost of cyber crime, 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 cyber crime 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, the economic impact of cyber crime cannot be comprehensively captured with those. The core problem is that it is currently impossible to generate trustworthy monetary estimates for the impact on a country or a sector. 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.

In order to develop the most comprehensive knowledge on the cost of cyber crime, considering only quantitative data is not enough. In this article we propose a flexible framework for capturing information that gives the chance to fill the gaps on the cost of cyber crime knowledge arising from both possible missing quantitative and qualitative data. Our framework follows a mixed top-down/bottom-down methodology as it aims to break down the whole complex phenomenon of the impact of cyber crime and have a more specific and in-depth view, analyzing its sub-components. This methodology focuses on macro economic units of analysis and tries to move from the general view to the smallest and more specific sub-components.

Existing frameworks to measure the cost of cyber crime have mainly focused on specific cyber incidents and mostly adopted a bottom-up methodology (e.g., [32]). We argue that due to the lack of accurate data, bottom-up methodologies are not appropriate as

The research leading to these results has received funding from the Specific Programme "Cooperation": Security of the European Union's Seventh Framework Programme FP7/2007-2013/ under REA grant agreement 607775.

NSPW'17, Islamorada, Florida, USA

DOI: 10.1145/nnnnnnn.nnnnnnn

they are focused on one side of the problem. Similarly, top-down methodologies are suitable for measuring the level of cyber crime in each country but they fail to capture the impact at the agent level. Our framework captures both short-term agent level impacts and also long-term distortionary effects of cyber crime. We aim at measuring the impact of cyber crime by means of several indicators and variables regarding not only the impact on specific agents but also industry sectors, law enforcement effectiveness and impact upon society.

At the short-term agent level impact, our framework considers three different costs categories: the costs in *anticipation* of cyber crime, as a *consequence* of cyber crime and in *response* to cyber crime. The first category covers all types of expenditures occurring before the cyber incident; the second one refers to all costs directly connected to crime events; lastly, the third one encompasses all costs incurred in response to crime. As long-term distortionary effects, our framework includes market frictions and inefficiencies, innovation deceleration, consumer avoidance, effects on competition and tax distortions. Thus, our framework can be used to create estimates not just for agents directly suffering the cyber incident but for the society as a whole.

The remainder of the paper is organized as follows. In section 2 we provide a brief overview of the different approaches and methodologies for estimating the cost of cyber crime. Then, in section 3, we present the economic foundation of our framework and its different constituents. Finally, in section 4 we conclude the paper.

2 RELATED WORK

Literature around the cost of cyber crime is relatively small but growing as cost estimates become an integral part of any empirical-based risk management framework. Because of the small size of empirical research in this area, there is a large variance in estimates for the same time of cyber crime both at the country and sectoral level. The amount studies that attempt to generate estimates for a wide variety of common cyber crimes are in the best cases limited, but often present significant biases.

There are a few studies on the cost of cyber crime that provide parts of a comprehensive assessment. Either they focus on articulating a model to enumerate the different impacts (e.g., [15]), or on estimating only specific impacts based on a specific data set, such as data breaches (e.g., [27, 39]) or consumer losses related to malware [37]. Only a handful attempts try to empirically and systematically estimate the cost of cyber crime by: (i) presenting a model or framework to systematically identify the impacts; and (ii) using data from a variety of sources to estimate the impacts, either at the national or at the global level. An example of these are the reports of McAfee [17] and Detica [5]. They bring the partial estimates together into some overall monetary amount. However due to the lack of data, the numbers are based on murky calculations that outsiders cannot verify and that have been widely criticized [1]. The only alternative we know of is the study by Anderson et al. [1]. This presents a framework that identifies direct, indirect and defense costs. Rather than adding up the partial estimates, they argue it is more informative to present these impacts separately. This work represents the first step towards understanding the economic cost of cyber crime but overlooks crucial long-term economic distortions that can easily overshadow the monetary costs.

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 frameworks have to operate.

Any assessment of the economic impact of cyber crime needs three core ingredients:

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

In the following, we focus on the first and third ingredients, i.e., data and models to estimate the impact of cyber crime. The second ingredient, methods to associate events with economic impacts, is not specific to cyber crime, so we will not survey those methods. We refer the interested reader to sources that provide a survey of approaches to estimate economic value [3].

2.1 Cybercrime cost estimates from empirical data

Currently, different types of empirical data — that is, observable events — are being collected and used to create 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 [21]. This data is not available, however, for independent research. Furthermore, the market for cyber insurance is still too small to give a representative view of many different types of events.

However, these data sources suffer from the well-known difficulties in measuring cyber crime [9]. Lack of standardization, lack of understanding, under-reporting and over-reporting are a few of the issues that drive the estimates when assessing the impact of cyber crime. These constitute an endemic problem that propagates across different actors collecting cyber crime data. Our framework is agnostic to this issue as its ultimately purpose is to assess the economic impact in itself and not in monetary terms.

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 cyber crime. Everyone understands that some of them are mainly produced for sensationalist headlines. The infamous $1 trillion figure was published by the security company McAfee [17], 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 [16].

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) [17]. 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" [17, 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" [17, 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 [37]. 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 cyber crime 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 [9]. "No, it appears not," is their answer, after an extensive analysis of existing cyber crime surveys.

The set Ponemon surveys [23–28] are arguably among the better ones, but the problems are still immediately clear. First of all, the damage is mostly 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 cyber liability insurance claims where there was a data breach. Their finding was that the average loss per record was $0.56 [39]. 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.

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 organization. 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.

With their insistent talk about data, these reports 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.

2.2 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: generalization and aggregation.

Generalization concerns the issue of translating from the observed events and their impacts to an estimate of all events of that type and their impacts. Surveys of financial losses by organizations 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 organizations. Some research in this area has attempted to generalize the impacts of a handful of cyber incidents using simple models [6, 32].

As outlined by Florêncio and Herley [9], 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 generalization 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 totaled $560 million [13] in the US alone, while McAfee estimated a $1 trillion global cost [14].

The second issue is aggregation. Even when generalization 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 criticized for it [1, 9, 33, 36]. 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. Note that this wealth transfer does not have to happen among firms with on-line presence, as customers might decide to reduce their on-line activities and carry their business off-line.

There is a need for a framework that can identify and systematically aggregate these different impacts into a comprehensive assessment. Very few references exist that are sector-specific. In the financial services sector, for instance, Lagazio et al. [15] developed a multi-level model, based on system dynamics methodology, to understand the impact of cyber crime on this sector. Similarly, Nagurney [20] proposed a network economic model of cybercrime with a focus on financial services. Apart from these models for the financial services sector, no other comprehensive sector-specific model has been specified to estimate the cost of cybercrime.

Our framework is not sector specific and aims at identifying different economic impacts of cyber crime both in a short-term and long-term. It differs from previous approaches in several ways. 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, let's say among thousands of firms, will not solve the issue of generalizing from them to the larger aggregates of sectors, let alone countries or the world. Even a single sector in a single country harbors a large heterogeneity that would need large samples to accurate capture. Other data sources present other constraints that are equally persistent. Measurement of attacker behavior 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 our framework, this means that it has to be able to work under the existing constraints of available data. We think the framework of Anderson et al. [1] deals relatively well with these constraints. We follow their approach in enumerating and estimating a number of impacts. The most important departure from their approach, and from the other existing frameworks, is that we will distinguish more precisely between agent-level impacts (i.e., firm, organization, consumer) and societal impacts. All existing frameworks treat the overall societal impacts as the accumulation of agent-level impacts. As we will discuss in the next section, some costs to organizations are not societal losses, but rather wealth transfers of one organization to another. A simple example is customer churn after disclosing a data breach. This is a cost to the affected organization, but a gain to its competitors, who will receive the defecting customers. This can therefore not be considered 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 cyber crime.

This different starting point also means we have to adapt the taxonomy of cost impacts that the framework needs to articulate. Rather than following the set of impacts that Anderson et al. [1] identified, we will use an approach similar to Brand and Price [2], 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 organizations who suffer from the consequences of cyber crime.

3 A FRAMEWORK FOR THE ECONOMIC IMPACT OF CYBER CRIME

Previous cost-of-crime studies have routinely violated basic economic principles as a result of the many complexities and problems associated with assessing the economic impact on our societies. In this section we provide a framework that brings together the various impacts of cyber crime at different levels of society, and does so while adhering to economic principles. Before going into the details of our framework, first we review the economic principles and foundations this framework is built upon.

3.1 Economic principles and foundations

Estimating the total cost of cyber crime is a daunting task that would require to account for any distortion that cyber crime induce to the economic welfare. studying the various effects of cyber crime 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 cyber crime in two dimensions: (i) the various types of costs, classified by their relation to actual cyber crime incidents; and (ii) 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 framework that effectively breaks down the problem of estimating the impact of cyber crime into smaller subproblems which are more amenable to detailed analysis.

In developing our framework we draw upon a century of research on the cost of crime. While cyber crime is a modern invention, set

apart from traditional crime in such matters as its highly transboundary character and the problems of attribution, analyzing its impact requires the same economic ideas. Indeed, some of the fallacies and methodological difficulties that tainted previous reports on the costs of cyber crime were already pointed out by criminologists Hawkins and Waller [11], some 80 years ago. What follows now is a short review of several relevant principles of economics.

3.1.1 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 maximize welfare. Cyber crime 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, cyber crime 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 billion revenue in 2014 [34] — is evidence of this: the resources poured into these products could also be used to develop new technology, if there were no cyber crime.

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. 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.

3.1.2 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 cyber crime 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.

For instance, Huygen et al. [12] 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-cyber crime studies have failed to understand this, and estimated the total societal impact of cyber crime 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.

3.1.3 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. 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 symbolizes 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 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 behavior in response to the strain of cyber crime. For instance, consumers may avoid online services like banking and shopping for fear of cyber crime [31]. Likewise, businesses may invest less in research and development, thinking that hackers would steal their innovations. The economic inefficiencies introduced by such behavioral changes form part of the costs to society.

In our framework 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 classify the short-term effects that impact individual actors. We then discuss the long term economic distortions that these effects bring upon sectors, nations, and the society as a whole.

3.2 Short-term impact of cybercrime to individual agents

We proceed now by listing the various costs of cyber crime to individual economic agents, as well as the costs brought about by their collective efforts against cyber crime. This classification breaks up the economic impact assessment by identifying different types of losses and expenses that can be measured and estimated separately. The practical advantage of this typology is that each cost type can be studied on its own.

We further classify the various cost types as either costs in *anticipation* of cyber crime, costs as a *consequence* of cyber crime incidents, or costs of *response* to cyber crime. The first two categories include all losses and expenses made by victims or potential victims. The response category includes expenditures on public or private sector efforts taken to fight cyber crime.

A similar classification was used in several cost-of-crime studies, e.g. Brand and Price [2] and Czabanski [4]. Our typology of costs as a consequence of cyber crime incidents closely resembles earlier work by van Eeten et al. [38].

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 estimable losses and expenses. The ultimate cost of cyber crime to a sector or nation 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.

Consequence.

- **Stolen funds.** These include 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 [19], 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 behavioral 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 cyber crime is no exception. If we were to analyze 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,

Figure 1: Framework to assess the economic impact of cyber crime

Short-term agent-level impacts		
Anticipation	**Consequence**	**Response**
Expenditure on security services and products Productivity losses due to security policies Costs of security assessments Insurance costs	Stolen funds Pain and Suffering Cost of disruption Repair costs Reputation damage and customer attrition IP loss	Criminal Justice System Cost of awareness initiatives CSIRTs

Long-term distortionary effects		
Consumer avoidance Slowing down of innovation	Market frictions and inefficiencies Effects on competition	Tax distortions

and often have spill-over effects on organizations 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, publicized 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. [1], 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.

The impact of cyber crime goes beyond the consequences inflicted after a cyber attack and also imposes significant costs to the criminal justice system. These include expenditures on police and other law enforcement agencies, prosecutors, judges (in criminal courts), prisons and other correctional facilities, probation officers, etc. Moreover, national and local Computer Security Incident Response Teams (CSIRTs) have to be created to manage cyber attacks. But not only that, society also spends money on crime prevention such as awareness campaigns.

- **Criminal Justice System.** All costs made by the CJS — police, prosecutors, courts, and the correctional system. Also included are costs for witnesses and suspects.

  In addition, law enforcement agencies sometimes make efforts to prevent cyber crime. This includes activities like surveillance and monitoring of communication channels and disrupting online markets that facilitate cyber crime [8].
- **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.
- **CSIRTs.** Computer Security Incident Response Teams (sometimes called Compute Emergency Response Teams or similar variants) are primarily 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 other services such as security consulting and awareness building.

Traditionally, the costs of society's response to traditional crime were estimated by the law enforcement agencies' budgets. However, in the case of cyber crime these will only represent a lower bound estimate of the society's. Often, boundaries between cyber crime reducing efforts and other activities are blurred. For instance, probation officers and lawyers do not exclusively handle cyber criminals. Table 1 shows the main response costs and the parties that bear the cost. Though most of the response costs are borne by the society, offenders and victims also suffer from the society's response. Furthermore, as the criminal justice system is funded by

the taxpayer, the impact of the society response also causes long term distortions on the economy. Society losses go beyond the mere amount of taxes.

Costs	Party who bears the cost
Police	Society/government
Prosecution	Society/government
Courts	Society/government
Legal fees	
– Public defenders	Society/government
– Private lawyers	Offenders
Criminal sanctions	Society/government
Victim and witness costs	Victim/Witnesses
Jury service	Jurors
Victim compensation	Society/government
Offender costs	
– Productivity	Offender/society
– Injury/death to offender while incarcerated	Offender/society
– Loss of freedom to offender	Offender
– Offender's family	Offender's family/society
Over deterrence costs	
– Innocent individuals accused of offenses	Innocent "offenders"
– Restrictions on legitimate activities	Society
– Costs of additional detection avoidance by offenders	Offenders
Justice costs	Society
CSIRTs	Society/government

Table 1: Taxonomy of crime costs – response to crime (extended from [3])

One of the most prominent responses to cyber crime is the creation of Computer security incident response teams (CSIRTs). CSIRTs are commonly used by large companies and government agencies to help mitigate cyber threats and insulate them from future attacks. The costs of building and operating the CSIRT will depend on the number and types of services provided [35], as well as: the size of the constituency they are provided to; the administrative costs for the area or organization; and the structure of the CSIRT. Infrastructure costs and salary/wages/benefits are the largest costs of a CSIRT. Besides staff and infrastructure costs, CSIRTs also require equipment expenditures and training.

3.3 Long-term distortionary effects of cybercrime

The costs listed above characterize 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.

Consumer avoidance

Cyber crime may cause consumers to avoid using services such as online banking or online shopping. This avoidance could be the result of a level-headed 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 [10, 30].

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 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, labor 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. [7] 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 authentication. 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 emphasize 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 behavior of economic agents, in such matters as consumption and labor-leisure trade-offs. 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: (i) 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 (ii) 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 trade-off between access and incentives for innovation is reflected in patent rights, for example, which protect IP owners but only for a limited period [29]. 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 organizations. The magnitude varies based on sector, organization 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" [22].

4 CONCLUSIONS

The impact of cyber crime goes beyond the consequences inflicted by a cyber attack and imposes significant costs to the well-functioning of an economy. Currently there exists a lack of guidance to estimate this impact and the dearth of research on this area creates a knowledge gap. Over the last decade, numerous industry reports have attempted to fill this gap by creating monetary estimates. Additional research effort has made considerable progress by providing some calculations specific for some cyber crimes. However, most of these calculations have been widely criticized as the principal methods used to generate cost estimates may be biased both upwards and downwards. Only a handful of research studies have made a serious effort to systematically estimate the cost of cyber crime, though none of these succeed to include the distortionary effects into their estimates.

In this paper, we propose a framework based on several indicators that serve as guidance to assess and measure the impact of cyber crime. Therefore, this list of indicator should be considered as a starting point to be used for addressing a future more specific analysis on this topic. Nevertheless, this paper aims to be a generic framework rather than a list that could be completely filled out nowadays. At the same time, it helps to direct data collection, explaining which indicators can satisfy basic information on any of the impact of cyber crime. To be effective, economic impact assessments require the systematic collection of accurate and reliable information based on the factors and indicators that our framework identifies.

While some factors are relatively easy to estimate, others are virtually impossible. The current chronic lack of data in relation to the long-term distortionary impacts of cyber crime provides enormous scope for future research. Only with better data –not only about the agent-level costs of cyber crime but also about social impacts– will better decisions on cyber security investment be possible.

REFERENCES

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

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

[3] M.A. Cohen. 2004. *The Costs of Crime and Justice.* Taylor & Francis.

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

[5] Detica and Office, Cabinet. 2011. 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).

[6] Thomas Dubendorfer, Arno Wagner, and Bernhard Plattner. 2004. An economic damage model for large-scale internet attacks. In *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2004. WET ICE 2004. 13th IEEE International Workshops on.* IEEE, 223–228.

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

[8] Nick FitzGerald, Ian Whalley, Richard Ford, and Edward Wilding. 2007. Darknet Monitoring. *Virus bulletin* (2007).

[9] Dinei Florêncio and Cormac Herley. 2013. Sex, lies and cyber-crime surveys. In *Economics of information security and privacy III.* Springer, 35–53.

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

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

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

[13] Internet Crime Complaint Center. 2010. 2010 Internet Crime Report. http://www.ic3.gov/media/annualreport/2010_IC3report.pdf. (2010).

[14] K Kannan, Jackie Rees, and EH Spafford. 2009. Unsecured Economies: Protecting Vital Information. *Red Consultancy for McAfee, Inc* (2009).

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

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

[17] McAfee. 2014. 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).

[18] McAfee and SAIC. 2011. Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency. http://www.ndia.org/Divisions/Divisions/Cyber/Documents/rp-underground-economies.pdf. (2011).

[19] D. Modic and R. Anderson. 2015. It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security Privacy* 13, 5 (Sept 2015), 99–103. DOI: http://dx.doi.org/10.1109/MSP.2015.107

[20] Anna Nagurney. 2015. A multiproduct network economic model of cybercrime in financial services. *Service Science* 7, 1 (2015), 70–81.

[21] NetDiligence. 2014. Cyber Claims Study 2014. http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf. (2014).

[22] Dave Pelland. 1995. Outsourcing: More efficient risk management? *Risk Management* 42, 5 (1995), 56.

[23] Ponemon Institute. 2013. 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).

[24] Ponemon Institute. 2014. 2014 Survey on Medical Identity Theft. http://mededfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_

Theft_Study1.pdf. (2014).
[25] Ponemon Institute. 2015. 2015 Cost of Cyber Crime Study: Global. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/. (2015).
[26] Ponemon Institute. 2015. 2015 State of the Endpoint Report: User-Centric Risk. http://www.ponemon.org/local/upload/file/2015INAL.pdf. (2015).
[27] Ponemon Institute. 2015. Cost of Data Breach Study. http://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF. (2015).
[28] Ponemon Institute. 2015. The Cost of Phishing & Value of Employee Training. http://info.wombatsecurity.com/hubfs/Ponemon_Institute_Cost_of_Phishing.pdf. (2015).
[29] Richard Posner. 2005. Intellectual Property: The Law-and-Economics Approach. *Journal of Economic Perspectives* (Jan. 2005), 57. http://chicagounbound.uchicago.edu/journal_articles/310
[30] Markus Riek, Rainer Boehme, Michael Ciere, Carlos Gañán, and Michel van Eeten. 2016. Estimating the Costs of Consumer-facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries. In *Workshop on the Economics of Information Security (WEIS)*.
[31] M. Riek, R. Bohme, and T. Moore. 2015. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *Dependable and Secure Computing, IEEE Transactions on* PP, 99 (2015), 1–1. DOI: http://dx.doi.org/10.1109/TDSC.2015.2410795
[32] Sasha Romanosky. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity* 2, 2 (2016), 121.
[33] Julie J. C. H. Ryan, D. Sc, and The George. 2003. The Use, Misuse, and Abuse of Statistics in Information Security Research, Presented to American Society of Engineering. In *Management National Conference (ASEM 2003)*.
[34] Sid Deshpande and Ruggero Contu. 2015. *Market Share Analysis: Security Software, Worldwide*. Technical Report. Gartner. https://www.gartner.com/doc/3341217/market-share-analysis-security-software.
[35] Software Engineering Institute. 2016. CSIRT Services. http://www.cert.org/incident-management/services.cfm. (2016).
[36] Darlene Storm. 2014. $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).
[37] 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).
[38] Michel van Eeten, Johannes Bauer, and Shirin Tabatabaie. 2009. Damages from internet security incidents. A framework and toolkit for assessing the economic costs of security breaches. *Delft University of Technology, The Netherlands* (2009).
[39] Verizon. 2015. Data Breach Investigations report. https://its.ny.gov/sites/default/files/documents/rp_data-breach-investigation-report-2015_en_xg.pdf. (2015).