Home Office

Understanding the costs of cyber crime

A report of key findings from the Costs of Cyber Crime Working Group

Research Report 96

Home Office Science Advisory Council

January 2018

Contents

Acknowledgements

Home Office Analysis and Insight provided support to the Home Office Science Advisory Council (HOSAC) in setting up and running the Costs of Cyber Crime Working Group between Autumn 2014 and Spring 2016. This report was written by Anthony Cooper and Samantha Dowling from Home Office Analysis and Insight, on behalf of HOSAC. Co-ordination of the Working Group was led by Samantha Dowling, with support from Tom Bucke, Sam Brand, Rob Street, Sophia Hinde, Sean Mills and Angie Scholes.

The authors would like to thank the external members of the Costs of Cyber *C*rime Working Group: Professor Dave Delpy, Professor David Wall, Professor Steve Furnell, Professor David Pym, Ruth Davies, Ali Imanat, Dr Tom Holt, Dr Alice Hutchings, Emma Dickens, John Flatley, Patrick Anderson, Gareth Rees, David Fyson, Tom Ryder, Henry Bryers, and DI Chris Felton for their contributions to the Working Group. Thanks are also owed to the various other researchers who conducted original research to address identified knowledge gaps: Dr Adam Bossler, Professor Matt Williams, David Emm, Dr. Maria Papadaki, Dr. Olga Smirnova, Dr. Max Kilger, Caitlin Connors, Deborah Willis, Gurprit Dhillon, Catherine Grant and Preriit Souda. Finally, thanks are owed to colleagues in Home Office Analysis and Insight who supported this work programme, without whose help this report would not have been possible.

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).

Executive summary

Previous Home Office estimates of the costs of crime have historically excluded cyber crimes due to the challenges in developing robust estimates (Home Office, 2000), but there is increasing need to look at these more modern crime types to get a better understanding of their costs and harms. In broad terms, it is important to understand:

- where different costs fall (for example, in terms of cyber crime prevention, or in response to cyber crime);
- what forms the costs take; and
- who are most affected (for example, which individuals, which business areas).

The Serious and Organised Crime Strategy (Home Office, 2013a) therefore made a commitment to form an external Working Group to help to improve the quality of data associated with the costs of cyber crime. This report does not attempt to arrive at an overall estimate of the cost of cyber crime. Rather, it outlines the activity of the Costs of Cyber Crime Working Group to improve data quality in this area, specifically focusing on the development of an overarching framework for estimating costs. In the light of this framework this report makes a number of recommendations on the design of future research into the costs of cyber crime. This report is therefore intended to help to take the research community closer towards achieving better estimates of the costs of cyber crime as part of future studies.

The Costs of Cyber Crime Working Group involved academics, officials from a number of government departments and representatives from law enforcement and other industry bodies responsible for helping to tackle cyber crime. Governance for the Working Group rested with the Home Office Science Advisory Council (HOSAC). The Working Group was in operation between Autumn 2014 and Spring 2016. The remit of the group covered cyber-dependent crimes (e.g. spread of malware, hacking and DDoS[1] attacks) and cyber-enabled crimes (e.g. fraud and theft) as defined by the Serious and Organised Crime Strategy (Home Office 2013a). The remit also included both individuals and businesses / organisations as victims.

Over the 16-month duration of the Working Group a number of research studies were conducted to help to address specific evidence gaps and challenges associated with

[1] Distributed Denial of Service attacks, see Home Office 2013c.

developing cost estimates. These studies included analysis of previously underused data sources and generated the following key findings.

- A new estimate of £1.6 million in costs to the UK Government and industry targets from a sample of 1,250 web defacements[2] occurring between 2007 and 2015, with an average cost per defacement of approximately £1,200.[3]

- A new estimate of £5.1 million in costs to UK-based companies of 89 malware infections reported to the Malware Domain List[4] between 2009 and 2014, with an average cost per infection in excess of £57,000.[5]

- New estimates of between £6.1 million and £25.2 million for how much buyers of stolen financial data earned when exploiting card data purchased from the open and dark web. Estimates were derived from a sample-based study investigating the use of stolen data that were purchased in dumps of 50 sets of card details.

- New median estimates of earnings to sellers of stolen financial data[6] of between £89,000 and £355,000. Within a dark web sample, sellers earned between £24,000 and £95,000 at the median price.

- A set of new survey measures for helping to gain a better understanding of business reputation costs from cyber crime, alongside practical guidance for businesses in helping to identify and mitigate the impacts from potential reputational damage.

- The finding that fear of cyber crime has a measurable 'soft' cost. Analysis found that within the EU, Great Britain is placed the sixth most fearful of economic cyber crimes and the fourth most fearful of content cyber crimes. The burden of fear is greater for economic cyber crime than for content cyber crime. Victims, women, parents and the economically disadvantaged are significantly more likely to fear cyber crime.

It is worth noting that the new figures identified by the studies presented in this report are based on research using samples of available data, and are a small element of the likely total costs.

A framework (which split costs into: costs in anticipation, costs as a consequence and costs in response) was developed to help to conceptualise the full range of cyber crime costs and set out how other researchers might approach future cost estimation. A review of previous

[2] Web defacements refer to hackers modifying the original homepage of a site with content and messaging of their own design, to satisfy a variety of motivations.

[3] Though it is important to note that the cost is variable from year to year, so this is not a static figure. Estimate drawn from sample of reports made to website defacement repository, Zone H.

[4] Focusing on malware infections reported at the server level only, within the UK.

[5] Though it is important to note that the malware type affects individual costs and costs vary by year, meaning that the exact costs per infection may differ from this average value.

[6] This study considered stolen financial data consisting of lots of 50 sets of card details.

costs of cyber crime research found that many studies failed to identify clearly the range of different costs associated with cyber crime. They used inconsistent definitions of both costs and cyber crime, and most studies simply did not measure the same thing making comparisons between studies very difficult. For example:

- some studies measured cost per incident, while others measured cost per year or cost per victim;
- similarly, some studies included large costs for intellectual property theft, while other studies considered this to be out of scope.

As such, one of the main aims of the framework was to address the fundamental challenge of what should, ideally, be measured.

Understanding the scale or prevalence of cyber crime is also a key requirement for estimating the costs. A number of wider developments occurred during the course of the Working Group - and since its completion – which have subsequently improved the quality of available data on scale. This includes the new experimental measures on cyber crime produced by the Office for National Statistics (ONS) via the Crime Survey for England and Wales (CSEW); and also the Department for Culture, Media and Sport's (DCMS) Cyber Security Breaches Survey. Whilst these new data were not available for use during the course of the Working Group, it is important that developments such as these are incorporated into future work for assessing the costs of cyber crime.

Although it is encouraging that work to address many of the issues identified in this report are ongoing, it is important that momentum is maintained. This report therefore makes a number of recommendations, as listed below.

- Researchers designing future costs of cyber crime studies should: approach their research design in a systematic fashion; identify gaps in the costs of cyber crime framework; and tailor research questions so that they can fill these specific gaps.
- Future research should focus on the most notable gaps (for example, law enforcement costs) in the costs of cyber crime framework.
- Future studies should further investigate the costs and profits to offenders of engaging in cyber crime.
- Future studies should seek to test the measures presented in Appendix 3 of this report by investigating the financial impact of cyberattacks on the value of business reputation.
- Further depth analysis of Action Fraud data should be conducted to make the best use of the available cost data.
- Future research should further consider how to estimate the monetary cost of

the fear of cyber crime.

- Future studies should explore the use of increasingly robust survey data when estimating costs of cyber crime. For example, the CSEW measure of cyber crime and the DCMS Cyber Security Breaches Survey data.

1. Introduction

Various research studies over recent years have attempted to derive estimates of the costs associated with cyber crime. These studies have tended be inconsistent in their approach to estimating costs and as such have often adopted very different measures, for example, annual costs, costs per attack, costs per sector. Even where studies have taken a similar approach, the end results have often been inconsistent – for example, the Ponemon Institute (2015) estimated that the average annual cost of cyber crime to the UK public sector in 2012 was £1.2 million compared with the Detica's (2011) estimate that cyber crime cost the UK Government £3 billion per year. Furthermore, the widely quoted Detica/Cabinet Office research that estimated costs of £27 billion to the UK from cyber crime, received wide critique (for example, Anderson, *et al.,* 2012; Home Affairs Select Committee, 2013) drawing into question the reliability and accuracy of these types of estimates. The Home Affairs Select Committee (2013) more broadly expressed particular concern over the lack of accurate and up-to-date figures measuring the scale and cost of cyber crime.

In response to the various contradictory estimates of the costs of cyber crime presented in the literature, in the *Serious and Organised Crime Strategy* (Home Office, 2013a), the Government acknowledged that *"an accurate estimate of the scale and cost of cyber crime will probably never be established".* Within the same strategy, the Government made a commitment to set up a new external Working Group to improve the quality of data associated with the costs of cyber crime. As such, this report does not attempt to arrive at an overall estimate of the cost of cyber crime, rather, it reports on the efforts made by the Costs of Cyber Crime Working Group, operating under the oversight of the Home Office Science Advisory Council (HOSAC), to improve data quality, specifically focusing on the development of a framework to conceptualise how best to estimate costs as part of further research. This report relates to work conducted between Autumn 2014 and Spring 2016, it does not therefore include reference to all subsequent research related to estimating the costs of cyber crime published since then.

Whilst recognising how challenging it is to estimate the costs of cyber crime, the Working Group identified a number of important reasons for improving the data quality in this area. Developing a better understanding of both scale and costs is crucial to:

- understanding the nature of the cyber crime threat and how it is changing over time;
- raising awareness of cyber crime and its impacts amongst law enforcement, in order to help make informed decisions about priorities; and
- directing appropriate awareness raising and prevention initiatives towards those businesses and individuals who are most vulnerable.

In broad terms, it is important to understand where different costs fall (for example, in terms of cyber crime prevention, or in response to cyber crime), what form these costs take and who is most affected (for example, which individuals, which business areas).

A previous research report by the Home Office (2013c) noted that improvements in measurement and recording of cyber crime are *"critical to understanding whether the scale of cyber crime is increasing or decreasing and how the nature of the problem is evolving over time"* (p 14). And the National Statistician's 2011 *Review of Crime Statistics* (Government Statistical Service, 2011) expressed concern that existing statistics did not adequately capture cyber crimes. As a result of this, the costs of cyber crime work programme was being conducted during a time when a number of wider ongoing changes were being made to the data available on cyber crime to improve measurement and recording. The Office for National Statistics (ONS, 2015) also published a report on a field trial conducted to test new measures designed for inclusion in the Crime Survey for England and Wales (CSEW), to improve understanding on the scale and extent of fraud offences and cyber crime. Without such an understanding of the scale/prevalence of cyber crime offences, it is difficult to estimate robustly the overall cost of cyber crime.

The Working Group therefore took these developments into consideration, whilst seeking to avoid duplication. From October 2015 new cyber crime questions were included in the CSEW and for the first time in January 2017, these data were included in the overall crime count for the CSEW (ONS, 2017) resulting in an estimate of 2.0 million cyber crimes in England and Wales for the year ending September 2016. This now considerably improves understanding of the scale of these offences, but unfortunately the data were not available during the timescales of the Working Group. Similarly, the Department for Culture, Media and Sport (DCMS) revised its Cyber Security Breaches Survey for businesses, improving the methodological design and thus the robustness of resulting estimates, publishing new survey results for the first time in May 2016. Combined with other future developments, these improvements to the wider data sets available on cyber crime will likely serve to improve the quality of cost estimates in the future, but were unfortunately not available for use during the timescales of the Working Group.

The Costs of Cyber Crime Working Group

The Working Group was established in October 2014 and was made up of academics, officials from a number of government departments with an interest in cyber crime, and representatives from law enforcement and other bodies responsible for dedicating resources to tackle cyber crime. Governance for this Working Group rested with HOSAC and was chaired by a HOSAC member until its final meeting in March 2016.

The Working Group was tasked with setting the agenda and directing the work to be undertaken for improving data quality and estimates of both the social and economic costs of cyber crime. This includes work to improve understanding and measurement of:

- prevalence and/or incidence of cyber crime, which are necessary to improve cost estimates; and
- the wider non-financial harms and impacts of cyber crime, in addition to the financial harms.

The remit of the group covered cyber-dependent crimes and cyber-enabled crimes as set out in the Serious and Organised Crime Strategy and defined in Chapter 4. It also covered individuals, as well as businesses / organisations.

Over the 16-month duration of the Working Group a number of research studies were conducted:

- a review of the literature on the costs of cyber crime;
- developing a framework for estimating the costs of cyber crime;
- assessing the prevalence and financial impact of website defacement in the UK;
- assessing the scope and cost of malware infections within the UK;
- estimating profits and losses to underground markets;
- exploring the scale of reputational damage to businesses as a consequence of cyber crime;
- understanding the scale, trends and measurement of cyber-dependent crimes; and
- exploring the consequences of fear of cyber crime.

Summaries of the findings of these studies are presented in this report, alongside information on where to find more detailed write-ups, where these have been published by the researchers involved.

This report concludes with a discussion based on the developed costs of cyber crime framework, using the various learning points from the exercise to design this framework to inform directions for future research in this area.

2. Summary of the extant literature

i. Definitions

In the *Serious and Organised Crime Strategy* (Home Office, 2013a), the Government highlighted some of the issues arising from cyber crime, which it explained could be broken-down into two types of criminal activity:

> "*Cyber-dependent crimes: those which can only be committed using computers, computer networks or other forms of information communication technology (ICT).They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage*." (p 22).
>
> "*Cyber-enabled crimes: those which can be conducted on or offline, but online may take place at unprecedented scale and speed*." (p 22).

Examples of cyber-enabled crimes include fraud (including mass-marketing frauds, 'phishing' emails and other scams, and online banking and e-commerce frauds) and theft (including theft of personal information and identification-related data).

Other taxonomies and definitions of cyber crime exist, for example:

- Anderson et al. (2012) who used a definition that incorporates traditional forms of crime, publication of illegal content, and crimes unique to electronic networks; and
- Wall (2007[7]) who defined cyber crime as: crimes against the machine, crimes using machines and crimes in the machine.

However, in the interests of consistency with previous Home Office research, this report will consider cyber-dependent and cyber-enabled crimes.

The research presented in this report also does not examine the costs of cyber terrorism, online hate crimes, cyber bullying, digital piracy or online sexual crimes. The Costs of Cyber Crime Working Group agreed that these other types of costs should remain outside the remit of the group in order to ensure that the scale of the group's work was manageable and tightly focused, and also to avoid duplication with other work going on in these areas.

[7] Revised in May 2010 and February 2011.

ii. Costs of cyber crime

In order to understand the wide range of cost estimates reported in previous research findings, a literature review (by Dr Adam Bossler, in conjunction with Home Office Analysis and Insight) was conducted using an online search for UK cyber crime cost estimates that were published before 1 January 2016 dating back to the Detica (2011) report.

Overall, the review found that the extent and nature of estimated costs ranged from:

- a top-end estimate of £27 billion for economic costs to the UK (Detica, 2011);
- lower end costs for businesses, for example, of £4.1 million per year for 39 businesses (Ponemon Institute, 2015); and
- very specific component costs for example, £0.8 million in clean-up costs (Oxford Economics, 2014).

The studies also used a variety of methods, for example:

- scaling up/down based on 5 per cent of gross domestic product (GDP) (for example, Anderson *et al*., 2012);
- deriving estimates based on survey research (for example, Oxford Economics, 2014); and
- deriving estimates based on information reported directly by banks, in line with the agreed industry definitions and categories (for example, Financial Fraud Action [FFA] UK, 2015).

Furthermore, the studies used various units of measurement and types of costs, for example:

- economic costs (for example, Detica, 2011);
- average annualised costs (for example, Ponemon Institute, 2015);
- medians (for example, City of London Police, 2015);
- costs to the UK (for example, National Fraud Authority, 2013); and
- costs to businesses (for example, Detica, 2011).

The literature review highlighted a number of challenges associated with the cost estimates presented in the existing research literature. Many of the papers reviewed used differing definitions of the costs of cyber crime – this often meant that the studies were attempting to measure conceptually different things. This not only affected the resultant cyber crime cost impacts, but makes it difficult for researchers to meaningfully compare the different cyber crime cost estimates. In addition to definition differences, various studies in the literature attempted to measure very different types of cost, as well as different types of cyber crime. In some cases this meant that aspects of cyber crime simply went unmeasured – for example the Detica (2011) paper, which focused on a very narrow set of crimes.

A range of methods were used. Some studies used the costs in anticipation, costs as a response and costs as a consequence approach (for example, Anderson *et al*., 2012), other studies utilised a wide range of different methods, which lack comparability.

While some studies used surveys to provide data for their estimations, a number of these surveys were methodologically weak. For example, the Oxford Economics (2014) study did not utilise random probability sampling. Such methodological weaknesses in surveys have a number of implications, not least that it is difficult for researchers to extrapolate such findings to the wider population. However, even where random probability sampling is used, estimating losses from surveys is generally challenging, as many survey-based estimates of loss:

- are likely to represent just a fraction of the individuals/organisations surveyed;
- are based on unverified self-report; and
- may be skewed upwards by extreme losses reported by just a few respondents (Home Office, 2013c).

A large proportion of an estimate can often come from a handful of respondents, as the distribution of losses amongst the population is not likely to be experienced in a uniform manner (Florencio and Herley, 2011). In surveys where negative values are possible (for example, polling surveys) this error caused by uneven distributions of the phenomenon being measured can cancel itself out. However, in surveys where only positive values are possible (for example, surveys measuring cost) this is not true, meaning that while a lower bound is created there is no upper bound, so that "*bias is always upward*" (*ibid.*, p 2). Furthermore, where the phenomenon being measured is rare, non-response error can be considerable, meaning that the effects of incorrect data captured (for example, though lies, exaggeration and misrepresentation) can be difficult to gauge (*ibid.*, p 2).

A number of studies considered during the literature review were case studies. While such studies provide researchers and practitioners with useful context around the challenges of deriving cyber crime cost estimates, they do not allow extrapolation and are not necessarily representative of the wider cyber crime landscape. Even where random sampling approaches are used, the highly concentrated nature of cyber crime losses means that "*representative sampling of the population does not give representative sampling of the losses*" (*ibid.*, p 1).

In some of the weaker studies, a number of assumptions were made on which subsequent cost estimates were based. However, the theory underpinning such assumptions, and in some cases the assumptions themselves, were not always clearly documented. This makes it difficult for researchers to replicate such studies and means that subsequent estimates cannot be robustly verified.

Similarly, the review of the literature found that the methodological approaches and assumptions used by the researchers sometimes meant that it was difficult to establish how robust the resultant cost estimates were. An example of this is the approach used in the study by Anderson *et al*. (2012) to scale estimates based on the UK's share of world GDP. Using a broad approach such as this could result in some estimates being less robust than estimates derived through specific measurement of UK activity.

The review of the literature additionally recognised that a number of studies lack sufficient transparency to be able to robustly critique the methods and approaches used and to replicate the studies. In such cases, it is difficult to assess accurately the reliability and robustness of any measures generated.

Although no estimate of the overall cost of cyber crime, that could be interpreted with a high level of confidence, was identified in the literature, it was clear from reviewing the existing literature that some data were of relatively higher quality than other data and estimates. The data reported by Financial Fraud Action UK (2015), for example, likely represents some of the more reliable data currently available with which to begin to consider the overall cost of cyber crime to the UK. This is due to FFA UK collating information provided to them directly by various banks, regarding all their actual fraud cases and associated losses. The quality of these data is helped by the data sharing being conducted in line with agreed industry definitions and categories.

Based on the findings of this literature review, the work presented in the next chapter of this report focuses on a framework designed as part of this research programme to increase the quality of future research studies investigating the cost of cyber crime.

Table 1 provides a highlight summary of some of the key studies reviewed, along with an overview of some of the main cost estimates reported within those studies. The studies within Table 1 are presented in order of publication year, starting with the most recent. Where multiple papers were published within the same year, the studies have been presented in alphabetical order. A more detailed review of the literature is presented in Appendix 1 of this report.

Table 1 Summary of the key studies reviewed, 2011–Jan 2016

British Retail Consortium, 2015

Overview
"The British Retail Consortium (BRC) is the leading trade association representing the whole retail industry, from large multiples and department stores through to independents selling a wide selection of products through centre of town, out of town, rural, and virtual stores" (p 2). The BRC Retail Crime Survey aims to address the identified evidence gap created by the lack of a comprehensive measure of crime committed against UK businesses.

Within the report the authors define cyber crime as *"activity which utilises the internet to target data or other digital material or cases in which the primary motive of the attack is to disrupt systems or services"* (p 25). The authors noted that the majority of participating businesses said that cyberattacks *"remained a critical threat to their business"* (p 25).

Key cost estimates
The 2013–14 survey recorded 698,184 offences (not necessarily cyber-offences) against participating businesses that resulted in loss or damage to property. The authors noted that extrapolation based on this number indicated an estimated 3 million crimes (again, not necessarily cyber-offences) against the retail industry during the same period.

BRC (2015) reported that the total cost of crime to the UK retail sector was £603 million in 2013–14, which was an increase of 18 per cent compared with the previous year. The report also found that the majority of respondents indicated that the level of cyberattacks remained either the same or increased compared with the previous year.

In their chapter on fraud and cyber crime, the authors noted that a large proportion of fraud was committed online – particularly so for frauds that involved the theft of personal data. The participating retailers identified that *"the vast majority of credit/debit card fraud and one third of account credit fraud were committed online"* (p 23).

Key considerations
The BRC report authors did not provide detailed specifics on how their sample was created, but they stated that their *"sample covered 50 per cent of the retail sector by turnover and employed 1.6 million employees"* (p 10). Given the lack of detail available describing the research methods used, it is unclear how reliable the results generated by this survey are and how representative they are

of retail population as a whole, and, as such, whether the extrapolations made are valid.

Centre for Economics and British Research, 2015

Overview

The Centre for Economics and Business Research's (Cebr's) 2015 report provides information on how 201 C-suite executives (a colloquial term used to describe executives in senior management who tend to have the word 'chief' in their titles) viewed cyber security and the costs associated with cyberattacks.

Key cost estimates

Cebr estimated that cyberattacks caused a loss of £18 billion in revenue for UK firms as a result of the cyberattacks. In addition, they spent almost £16 billion in subsequent increased IT spending, in order to react to cybersecurity breaches.

Key considerations

The findings of this study are based on an online survey of 201 C-suite executives. It was not clear how the sample was selected, how representative the sample was of the wider population or how many of those approached responded to the survey. As such, it is not clear how generalisable these findings are.

City of London Police, 2015

Overview

In their (2015) report on the implications of economic cyber crime for policing, the authors focused on three main forms of economic cyber crime: cyber-dependent crimes, cyber-enabled crimes and cyber-assisted crimes "*differentiated from cyber-dependent and cyber-enabled crimes, and* [which] *use networked digital technologies (such as mapping applications) in the course of criminal activity which would take place anyway*" (p 3). In investigating these forms of cyber crimes the authors conducted original research on an extract of Action Fraud data, from which they reported a number of findings.

Key cost estimates

Examples of key estimates include the median amounts given to fraudsters by victims in the fourth quarter of 2014. For example, £38,974 for pension fraud, £28,609 for business trading fraud, £21,534 for financial investment fraud and £20,000 for bankruptcy and insolvency fraud.

Key considerations

While the research presented in this report provides a useful context when considering the types and magnitude of frauds reported, there are a number of technical and methodological considerations. For example, within the analysis, 'cyber-involvement' was determined based on the method of first contact, which may not be the most robust proxy. To provide an example of how this might not be the most robust proxy: using this definition 'hacking server' only has 31 per cent for the 'proportion of cyber-involvement', whereas given the nature of this offence it would be reasonable to expect 100 per cent cyber-involvement. As a further example, self-reported victim cost data were used within the analysis. However, these data need to be treated with caution as they are susceptible to misreporting, and reflect losses only at the time of initial reporting; they do not take into consideration subsequent compensation payments. Overall, this impacts on the level of confidence that can be attributed to the reported estimates, but represents a useful avenue for further exploration.

Financial Fraud Action UK, 2015

Overview

FFA UK provides regular reports on losses to the banking/payments card sector from various forms of fraud. These reports are collated from information provided by the banks regarding details of all their actual fraud cases and associated losses, in line with the agreed industry definitions and categories.

Key cost estimates

FFA UK reported that fraud losses on UK issued cards totalled £479 million in 2014, which was a 6 per cent increase from the previous year; £217.4 million of this total was e-commerce fraud and £60.4 million was online banking fraud.

Key considerations

The data reported by FFA UK likely represent some of the most reliable data currently available with which to begin to consider the overall cost of cyber crime to the UK. This is due to FFA UK collating information provided directly to them by banks, credit, debit and charge card issuers, and card payment acquirers in the UK regarding all their actual fraud cases and associated losses. These data are collected in line with industry agreed definitions and categories, and in addition to allowing the FFA UK to generate estimates, contribute to the discussion around how fraud is generally committed, and provide safety tips for consumers.

The FFA UK report lacks detail however, on exactly how the reported figures and costs are collected and tabulated. In addition, the report provided a summary of a number of measures that the card industry has taken over the last decade that have reportedly reduced the losses associated with fraud. For example, the Dedicated Card and Payment Crime Unit (DCPCU) is stated to have saved £470 million since its inception. No estimates were provided though on how much has been spent on these actions. Estimates on the costs of these measures would provide further knowledge on the anticipation/prevention costs of various forms of fraud.

Neustar, 2015

Overview

In its 2015 report, Neustar (a US-based global information services provider) presents the findings of its survey research of IT professionals, intended to assess current threats and business impacts of denial of service or distributed denial of service (DDoS) attacks.

Key cost estimates

In its sample of 250 professionals, Neustar (2015) found that 22 per cent of the companies reported losses between £50,000 and £99,999 per hour for revenue losses due to outages at peak times, making it the most common response option. For the rest 16 per cent reported that their losses per hour were less than £30,000; 12 per cent reported losses between £30,000 and £49,999; 16 per cent between £100,000 and £299,999; 11 per cent between £300,000 and £600,000; 12 per cent greater than £600,000; and 11 per cent did not know what their outages cost them.

Key considerations

It was not possible, from the information provided in the report, to gauge how representative these sample-based findings are of the wider population.

Ponemon Institute, 2015

Overview

The Ponemon Institute’s 2015 study of UK companies regarding the costs of cyber crime examined the total costs that organisations suffer because of cyberattacks. It included the detection, investigation and escalation, containment, recovery, ex post response and efforts to reduce the impact of the attack on information loss or theft, business disruption, equipment damage and revenue loss. The study is conducted on an annual basis and the reports looks at changes over time.

The Institute's methodology consisted of conducting 326 interviews of personnel in 39 large sized organisations. As the authors state in the report, *"each annual study involves a different sample of companies. In other words, we are not tracking the same sample of organisations over time"* (p 2). Therefore, differences in estimates from year to year may be differences in the organisations sampled rather than actual changes in costs.

Key cost estimates

The Ponemon Institute found that in 2015, the average annualised cost for the 39 corporations was £4.1 million per year (median of £3.4 million), a 14 per cent increase from 2014, with a range between £628,423 to £16 million.

Key considerations

It is specifically noted that the researchers' goal is not to provide estimates that can be generalised to the total costs of cyber crime on the UK economy but rather provide data on *"UK companies' experiences of cyber-attacks and on the broader 'cyber-attack landscape'"* (p 3). Some of the limitations include that Ponemon Institute (2015), similar to other companies, used its own confidential and proprietary benchmark method, which does not allow for outside scrutiny. In addition, its methodology consists of:

- a sampling plan that does not allow for statistical inferences;
- issues with non-response bias;
- a sampling frame bias in that it believed that it sampled companies with more mature information security programs; and
- reliance on the integrity of the respondents in providing the responses.

Verizon, 2015

Overview

In its 2015 report, Verizon (a US-based global technology company) was able to provide financial cost predictions for companies that had data breaches based on the number of records stolen. The report covered information on 70 contributing organisations in 61 countries during 2014. It detailed: 79,790 security incidents (defined as any event that compromises the confidentiality, integrity, or availability of an information asset); and 2,122 confirmed data breaches (defined as an incident that resulted in confirmed disclosure, not just exposure, to an unauthorised party).

Key cost estimates

The authors provide the predicted estimates of data breaches based on the size of the breach as measured by number of records stolen (100; 1,000; 10,000; 100,000; 1,000,000; 10,000,000; 100,000,000). For example, $1,258,670 is the expected financial costs to companies for a data breach with 1 million records stolen (the average was between $892,400 and $1,775,350 and the prediction between $57,600 to $27,500,090).

Key considerations

The authors noted that while they believe that many of their findings are generalisable, they cannot measure how much sample bias exists. They were unclear what proportion of all data breaches are represented as they did not know the total number of data breaches across all organisations – many such breaches go unreported or unnoticed.

McAfee/Intel, 2014

Overview

In the McAfee/Intel report (2014), the authors attempted to create estimates on the global cost of cyber crime, using existing estimates from previous studies. They write that their estimate: *"looks at both direct and indirect costs, and data used that take into account the loss of intellectual property,* *the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including the reputations damage to the hacked company"* (p 4).

Key cost estimates
The authors reported that the global cost of cyber crime is either $375 billion (considered conservative and estimated by extrapolating open source data), $445 billion (estimated by aggregating costs as a share of regional incomes), or a top estimate of $575 billion (extrapolating data from loss by high-income countries).

The McAfee/Intel report does not provide a UK cyber crime cost estimate. The authors reported that the proportion of UK GDP that is lost due to cyber crime is 0.16% – this proportion was given a low ranking of confidence.

Key considerations
As with all reports published by software producers/suppliers, readers need to be aware that such reports are produced to reinforce the need for/value of the products they offer. The research also draws chiefly on previous research studies, e.g. Anderson *et al* 2012, rather than produce any new primary research.

Oxford Economics, 2014

Overview
The Oxford Economics study produced an economic framework to understand the impacts of state-sponsored cyberattacks on UK firms. It carried out a survey of UK firms to estimate the cost impact of cyberattacks and an event study investigating the impact on market valuations of cyberattacks. It also included a number of case studies illustrating UK firms' experiences of cyberattacks.

The survey results presented in the report were based on an email/internet-based questionnaire sent to a database of IT professionals, IT security practitioners and other IT-related roles. In total, 9,973 surveys were issued and following screening, a response of 427 was achieved – a response rate of 4.3 per cent, which the authors comment was above the mean average for that industry. Given the sampling approach used, the survey results presented in this paper cannot be considered representative of the population of UK firms.

Key cost estimates
Example cost estimates provided in the report include the adjusted mean average UK firm cyberattack costs over 24 months prior to the survey: £0.8 million for clean up/remediation, £0.9 million for lost productivity, £0.8 million for disrupted operations, £0.8 million for damage/theft of IT and £0.9 million for reputation/branding.

The report additionally included median average UK firm cyberattack costs over 24 months prior to the survey: £0.18 million for clean up/remediation, £0.18 million for lost productivity, £0.18 million for disrupted operations, £0.18 million for damage/theft of IT and £0.38 million for reputation/branding.

Key considerations
The authors concluded that while the reported results of the survey are not generalisable, they might suggest that while only a minority of businesses suffer such losses, the cost of such losses are higher than other costs arising as a result of cyberattack.

National Fraud Authority, 2013

Overview

The National Fraud Authority (NFA) worked with stakeholders in various sectors and created overall estimates by collecting primary data through surveys and secondary data from its partners.

Key cost estimates

The NFA (2013) report estimated the cost of fraud to the UK economy at £52 billion. This figure, among many others in the report, is not broken down between online and offline fraud. The report estimates that charities were defrauded £147.3 million in both online and offline fraud, including payment fraud, fraud by employees or volunteers, and cyberfraud. Other estimates provided a little more insight into the proportion of the fraud type that was cyber-enabled. For example, the NFA estimated that the loss to financial sector for fraud per annum was £5.4 billion; £40 million of this was considered to be online banking fraud and £388 million was plastic card fraud. Individuals were estimated to have lost £9.1 billion as a result of fraud per year. The NFA divided this estimate into mass marketing fraud at £3.5 billion (much of it possibly being cyberfraud), identity fraud at £3.3 billion (much of which could also be cyberfraud), online ticket fraud at £1.5 billion (all cyberfraud), private rental property fraud at £755 million, and pre-payment meter scams at £2.7 million.

Key considerations

The NFA (2013) report noted that its estimates are not necessarily comparable from year to year because of improvements with methodology. Its estimates should therefore be viewed more as a *"best estimate of the possible size of the problem"* (p 4).

Furthermore, the estimates presented in the NFA report make use of:

- secondary data, not all of which are robust;
- data from non-random probability sample surveys, which are therefore unlikely to be representative of the population being researched; and
- mean average loss data, which are likely to be skewed by anomalies.

Symantec, 2013

Overview

Security software company Symantec similarly published cyber crime cost estimates as part of its 2013 *Norton Report* – a research study that examined consumer behaviours and the cost of cyber crime.

Key cost estimates

The authors reported that the global (based on 24 countries) total cost of cyber crime in the past 12 months was US$113 billion for an average direct cost per cyber crime victim of US$298. For the UK, they estimate that the total cost of cyber crime over the past 12 months was US$1 billion with an average direct cost per cyber crime victim of US$101. They estimated that there were 12m UK victims aged 18-64 in the 12 months prior to the survey.

Key considerations

The survey conducted in this work involved a small online UK sample – the usual limitations of generalisability to the wider population apply in terms of such survey approaches. As noted above, when interpreting reports published by software producers/suppliers, readers need to be aware that such reports are produced to reinforce the need for/value of the products they offer.

Anderson, Barton, Bohme, Clayton, van Eeten, Levi, Moore and Savage, 2012

Overview

To analyse the costs of cyber crime the report authors estimated global figures. In doing so, the authors worked on the assumption that the UK accounted for approximately 5 per cent of world

GDP to enable national estimates to be scaled up or down. The authors noted that where this approach was not suitable they would say so in the report and make *"an appropriate allowance"*.

Anderson *et al.* proposed an approach in which they split direct costs from indirect costs. Costs of security and social and opportunity costs of reduced trust in online transactions were also covered. The costs used in the analysis were taken from various international research, statistical sources and case-studies, and where necessary, assumptions were made by the report authors to arrive at the various costs estimated for the UK.

Key cost estimates

Anderson *et al*. (2012) estimated the total UK law enforcement expenditure on cyber crime to be $15 million. Additionally, the authors estimated that UK defence costs of firms generally cost $500 million and that the UK cost to users of clean up was also £500 million.

Key considerations

It is difficult to evaluate the reliability of a number of the cost values estimated. In part, this is because of the dependence on the work of others to arrive at component values used within the analysis. Although the paper represented an important step forward in setting out a more methodological approach / framework to assessing costs (Home Office, 2013c). Furthermore, limitations of this approach are outlined elsewhere as *'depending heavily on a GDP-based share of total crime costs to calculate UK estimates relies both on the accuracy of the global estimates used and the assumption that the relative proportion of an offending category in the UK is always equal in cost to its proportionate GDP'* (Home Office, 2013c).

It should be noted that the Anderson *et al*. report does not include figures for industrial cyber-espionage and extortion as *"there is no reliable evidence of the extent or cost of industrial cyber-espionage and extortion"* (p 18). Considering, however, that this estimate comprised a large proportion (£2.2 billion) of Detica's (2011) overall cyber crime cost estimate, the exclusion of cyber-espionage and extortion estimates in the Anderson *et al*. report partially explains the considerable difference in overall estimates.

Detica, 2011

Overview

This research focused on:

- identity theft and online scams;
- intellectual property (IP) theft;
- espionage and extortion; and
- fiscal fraud against the government.

The study was based on a snapshot of costs from 2010, and involved the development of a causal model, linking cyber crimes to their impact on the UK economy. This model was then used to map cyber crime types to categories of economic impact. This meant that the model could be used to calculate the magnitude of the costs of cyber crime using three-point estimates: worst-case; most likely case; and best-case scenarios.

Key cost estimates

The report concluded that in the most likely scenario, the estimated cost of cyber crime to the UK was £27 billion, with the authors noting that this was likely to be an underestimate.

Key considerations

There were a number of limitations associated with the Detica cost estimates. Many of these limitations relate to assumptions made by the report authors, which played a crucial part in arriving at the reported cost estimates. Example assumptions include:

- that only 1 in 15 incidents are reported by citizens;
- 25 per cent of identity fraud crimes are committed online; and
- all criminal attacks from the NFA Annual Fraud Indicator were cyberattacks.

Furthermore, a number of methodological decisions were taken in the Detica research that could affect the reliability of results. For example, the decision not to consider costs associated with IP-rich firms increasing their cyber-protection (as the authors considered these costs to be business-as-usual) and the decision to exclude costs borne by individuals in anticipation of cyber crime (for example, firewall, anti-virus software). Such considerations reinforce concerns with the reliability of the overall £27 billion cost estimate, as well as the various lower level estimates that contributed to this total.

3. Mapping the costs of cyber crime

i. Costs of crime

Costs of crime estimates can play an important role in helping the Government to achieve the greatest impact on crime for the money spent. The estimates can be used in both appraisal and evaluation of crime reduction policies. They can help the Government to prioritise, focusing scarce resources on policies that have the biggest impact on harm caused by crime, rather than simply the number of crimes (Home Office, 2000, p 7). The Home Office has previously published research examining the costs of traditional crimes such as burglary and violent crimes. The Home Office (2013b) also published a report estimating the social and economic costs of organised crime. However, due to the challenges associated with robustly calculating costs, cyber crime has not been included in any such estimates to date. In light of the emergence of new threats from cyber-enabled crimes and cyber-dependent crimes there is now a need to look at the impacts of new modern crime types and attempt to quantify the costs they pose to the UK economy.

The costs of crime work has taken an iterative research approach, and has published updates as methods and cost estimates have improved. This has enabled the cost of crime research to drive improvements in future research, as well as summarising the best-known cost estimates for the research community in an easy-to-access manner.

In calculating estimates, the costs of crime research has focused on the economic cost to the UK per incident, and has separately used estimates of the prevalence of crime in order to form an overall understanding of the cost of crime. Costs considered by this research have been broken down into three categories:

- costs in anticipation;
- costs as a consequence; and
- costs in response.

The methodological approach taken by the previous costs of crime research study has formed the basis of the approach taken in the costs of cyber crime research presented in this report.

ii. Economic concepts

In light of the lessons learned from the literature review exercise and a desire to promote consistency in future research, the Costs of Cyber Crime Working Group commissioned a project to devise a costs of cyber crime framework to summarise and understand better the different estimates of the costs of cyber crime. This project was undertaken by Dr Adam Bossler, in conjunction with Home Office Analysis and Insight. The framework approach was based closely on the Home Office's previous research investigating the costs of crime, and broke the costs down into the same three categories:

- costs in anticipation;
- costs as a consequence; and
- costs in response.

This chapter outlines the economic concepts behind the framework and then provides a description of the framework itself. Subsequent chapters of this report discuss how the framework could be used by researchers to ensure that future research studies are complementary and consistent in approach.

This project used the concept of economic cost to demonstrate the full impact of cyber crime on the UK economy. Economic concepts were taken from HM Treasury's 2003 *Green Book* guidance. A key economic concept used throughout the costs of cyber crime framework is that of opportunity cost. This relates to *"the value of the most valuable of alternative uses"*[8] essentially meaning the value of money or resource had it been used elsewhere instead of being attributed, in this case, to cyber crime. The concept of opportunity cost allows researchers to place a value on the resources, such as the people or money that will be freed up if there was no cyber crime present in the UK.

The concept of transfer payments and their place in the framework must also be considered. Transfer payments occur in an economy when there is no good or service received in return. This can include such transactions as subsidies or gambling. The costs of crime framework does not include transfer payments as they are not seen as a loss to society and are simply movements of money through the UK economy. Examples of transfer payments relating to the costs of cyber crime include fines handed out to companies for not properly securing data from cybercriminals, this is not seen as a cost to the economy and is seen as purely a financial cost to firms.

Furthermore insurance payments to victims of cyber crime are not present in the costs of cyber crime framework following guidance from the Home Office costs of crime work. This omitted insurance claims as the transfer of money between victims and insurance companies and compensation from insurance companies to victims was not seen as a loss to society. However, although insurance claims are not included in the costs of cyber crime framework, the insurance administration costs are. These are the costs of staff, premises and equipment that insurance companies face, and represent an opportunity cost to society as in the absence of cyber crime these resources would be freed up and used elsewhere in the economy.

iii Costs of cyber crime framework

As previously stated, costs have been classified into three categories to represent the distinct stages of how victims experience the costs of cyber crime:

- costs in anticipation of cyber crime;
- costs as a consequence of cyber crime; and
- costs in response to cyber crime.

[8] HM Treasury: *Green Book*, Glossary

Costs in anticipation are normally defensive measures taken by individuals and businesses to prevent crime. Examples would include expenditure on anti-virus software.

Costs as a consequence look at costs that occur as an immediate result of a crime, and normally takes the form of property damage or money lost. However it does also extend to the emotional and physical costs from crime. These are costs over which individuals have little, or no, control.

Costs in response look at costs that occur as a result of a decision regarding what to do in response to a specific crime. This typically involves responses provided by police forces and the criminal justice system, both of which feel a burden and suffer opportunity costs as a result of cyber crime. These are costs over which there is typically more control regarding what should be done.

The costs of cyber crime framework is an attempt to combine all that is known about the costs into one table that would enable greater understanding of current (as at 2016) research gaps and encourage further research. This intention was to enable researchers to identify what the various different component costs of cyber crime are, and how these combine to form the overall cost of cyber crime – a resource that did not previously exist in the extant literature. Considering costs in this way should help researchers to identify gaps for future research, facilitating the design of consistent research, which could be used together in future to get closer to understanding the overall cost of cyber crime. The framework, summarising a range of component costs, is outlined in Table 2. The cost types included in the framework were derived both from consultation with Home Office analysts and the Costs of Cyber Crime Working Group, with others advised by the literature review.

Table 2. The costs of cyber crime framework – summary of cost types

Costs in Anticipation

Technology costs

- Computer security protection software/products (for example, anti-virus, patching)
- Introduction of new/additional technologies

Training

- Cybersecurity training/education
- Training for law enforcement investigators and officers
- Training of court and legal personnel

Security practices/behaviours

- Implementing cybersecurity practices
- Usability/user impact as a result of increased security procedures
- Switching internet service providers (ISPs), security providers or products to increase security
- Vetting staff or contractors for security purposes
- Monitoring third parties' security
- Checking credit histories/scores
- Avoidance of the internet and/or other technologies (amongst non-users[9])

Government activities

- Drafting and creating new legislation
- Efforts to educate public on new legislation
- Implementation of national awareness raising/protection campaigns

Other

- Cyber-insurance administration
- Consumer credit/identity protection services (for example, CIFAS, a fraud protection organisation)
- Fear/worry about cyber crime
- Collection and compilation of cyber crime statistics

[9] Individuals who have never used the internet.

Costs as a Consequence

Costs of fixing an attack

- Equipment/infrastructure damage
- Clean-up expenditures
- Rectifying credit histories/scores

Financial losses

- Business disruption (including lost outputs)
- Online theft/fraud of funds
- Lost value of intellectual property/commercially sensitive information
- Damage to reputation or brand value
- Disputed transactions

Other

- Emotional/physical harms
- Victim support services

Costs in Response

Criminal justice system (CJS) responses

Law enforcement

- Law enforcement disruption and investigation activities

Courts

- Prosecuting cyber cases

Prisons and probation

- Additional costs to the probation system
- Incarceration of cybercriminals

Non-CJS responses

- Reporting/documenting incidents
- Legal, PR advice and similar expenses
- Increased/improved IT spending as a direct response to victimisation
- Training/education put in place as a direct response to victimisation
- Switching ISPs, security providers or products as a direct response to victimisation
- Reduction in research and development expenditure

The Working Group initially considered whether it was possible to populate the framework using the literature already published within the academic community and as identified in Section 4. The intention was that populating the framework with values taken from the literature would allow any gaps in knowledge to be identified. However, the estimates identified by the literature review were generally not regarded by the Group to be robust enough, or the right fit, to populate a framework looking at the costs of cyber crime to the UK economy. There were issues cited that included:

- methodological issues (for example, not measuring the right type of cost);
- incomparability due to differences in measurement or the omission/inclusion of certain cyber crimes such as intellectual property theft;
- lack of transparency of method; and
- the problems of estimating the impact on the UK criminal justice system.

A framework populated with these types of estimates was therefore felt to provide an inaccurate assessment of the overall picture.

The framework products (Table 2 and Fig 1) presented in this report are therefore unpopulated and do not contain any estimates. They are intended to identify areas of future research and be a useful tool for visualising the costs of cyber crime to the UK economy. The aim is to help inspire further research to begin populating the framework to increase understanding of the costs surrounding this particular crime area.

Consistent with the approach taken in the Home Office costs of crime work, values used to fill the gaps in the costs of cyber crime framework should be the economic costs of cyber crime to the UK per incident. These can then be used in conjunction with separate estimates for the volumes of the various different types of incidents per year. In addition to this, as reliable estimates are created, the framework will allow the monitoring of progress in building an evidence base in this area to advise future UK policy around cyber crime. Considering the impact of cyber crime on multiple fronts, the framework will also allow for the consolidation of information and data from existing resources in a variety of sectors, including, but not limited to, the Government, law enforcement, organisations, businesses, and non-profit organisations.

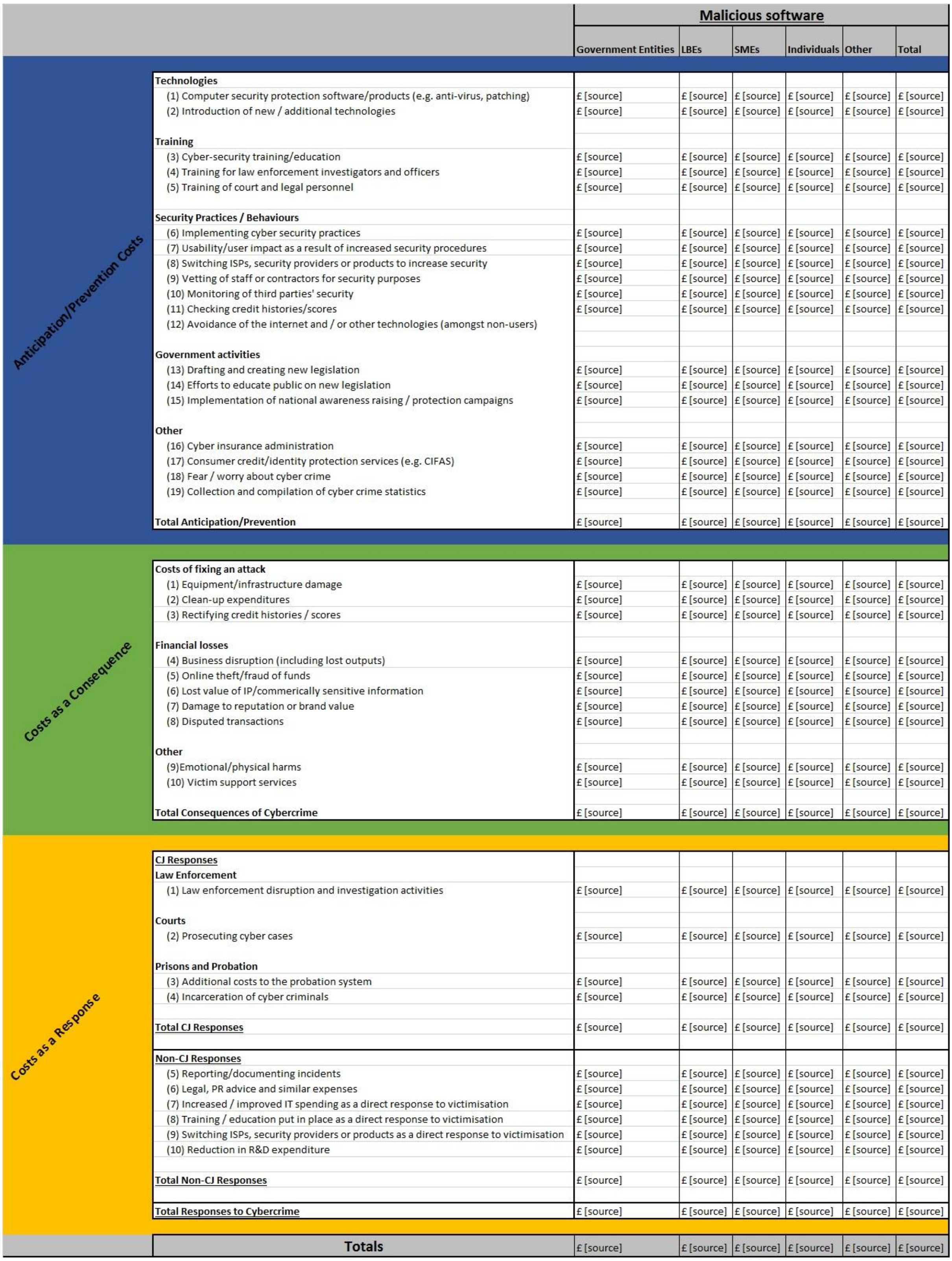
In the end, the costs of cyber crime framework is not meant as a final comment on exactly how cyber crime should be measured, but rather a starting point to help to indicate what is known and to provide possible future directions that scholars and agencies may wish to follow. It is important to note that some costs listed within the framework would still occur, even if there was zero cyber crime (for example, vetting staff or contractors for security purposes); as such, it is important that in future studies researchers isolate/attribute costs related to cyber crime.

An illustration of the costs of cyber crime framework

Fig 1 illustrates how the costs of cyber crime framework might look to researchers attempting to complete it in the future. The illustration highlights one column from the framework in relation to ‘malicious software’.

The framework consists of crime types across the X axis, broken-down by cyber-dependent crimes and cyber-enabled crimes. These are then split into four different economic actors (small and medium enterprises, large enterprises, government entities and individuals). The Y axis of the table shows the costs of cyber crime split into costs in anticipation, response and consequence. These are then split into smaller subcategories with specific costs placed into each one of these. For each cost item, the costs of cyber crime framework allows the placement of the estimate for an overall cyber crime category (for example, cyber-enabled) or specific form (for example, denial of service or distributed denial of service [DDoS] attack). In addition, readers will be able to examine cost estimates as they relate to the different economic actors that bear the costs of cyber crime. A glossary of key words used in the framework is presented in Appendix 2.

Figure 1. A sample illustration of the costs of cyber crime framework



		Malicious software					
		Government Entities	LBEs	SMEs	Individuals	Other	Total
Anticipation/Prevention Costs	**Technologies**						
	(1) Computer security protection software/products (e.g. anti-virus, patching)	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(2) Introduction of new / additional technologies	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Training						
	(3) Cyber-security training/education	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(4) Training for law enforcement investigators and officers	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(5) Training of court and legal personnel	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Security Practices / Behaviours						
	(6) Implementing cyber security practices	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(7) Usability/user impact as a result of increased security procedures	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(8) Switching ISPs, security providers or products to increase security	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(9) Vetting of staff or contractors for security purposes	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(10) Monitoring of third parties' security	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(11) Checking credit histories/scores	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(12) Avoidance of the internet and / or other technologies (amongst non-users)						
	Government activities						
	(13) Drafting and creating new legislation	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(14) Efforts to educate public on new legislation	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(15) Implementation of national awareness raising / protection campaigns	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Other						
	(16) Cyber insurance administration	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(17) Consumer credit/identity protection services (e.g. CIFAS)	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(18) Fear / worry about cyber crime	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(19) Collection and compilation of cyber crime statistics	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Total Anticipation/Prevention	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
Costs as a Consequence	**Costs of fixing an attack**						
	(1) Equipment/infrastructure damage	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(2) Clean-up expenditures	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(3) Rectifying credit histories / scores	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Financial losses						
	(4) Business disruption (including lost outputs)	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(5) Online theft/fraud of funds	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(6) Lost value of IP/commerically sensitive information	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(7) Damage to reputation or brand value	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(8) Disputed transactions	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Other						
	(9)Emotional/physical harms	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(10) Victim support services	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Total Consequences of Cybercrime	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
Costs as a Response	**CJ Responses**						
	Law Enforcement						
	(1) Law enforcement disruption and investigation activities	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Courts						
	(2) Prosecuting cyber cases	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Prisons and Probation						
	(3) Additional costs to the probation system	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(4) Incarceration of cyber criminals	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Total CJ Responses	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Non-CJ Responses						
	(5) Reporting/documenting incidents	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(6) Legal, PR advice and similar expenses	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(7) Increased / improved IT spending as a direct response to victimisation	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(8) Training / education put in place as a direct response to victimisation	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(9) Switching ISPs, security providers or products as a direct response to victimisation	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	(10) Reduction in R&D expenditure	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Total Non-CJ Responses	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Total Responses to Cybercrime	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]
	Totals	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]	£ [source]

4. Summary of findings from research commissioned by the Working Group

In addition to developing the costs of cyber crime framework, the Costs of Cyber Crime Working Group commissioned a number of discrete research projects to improve the quality of data required to understand the costs of cyber crime and begin to address identified knowledge gaps. These research projects were conducted by academics from a number of universities and faculties. This chapter provides a brief summary of the key findings of each of these projects; Appendix 4 signposts readers towards more detailed published reports.

i. Assessing the prevalence and financial impact of website defacement in the UK

The aim of this study, conducted by Dr Max Kilger and Dr Tom Holt, was to assess the prevalence, nature and financial impact of website defacement of business and individual websites in the UK. In addition to estimating cost, this study explored whether factors observed in the content of website defacements can be used to predict the costs of attacks.

Website defacement is one of the older forms of malicious online attacks, involving the replacement of a website's main page with images and content of the attacker’s choosing. Though defacements may not be as harmful as malicious software installations or a data breach, attacks may still be costly, particularly if there are less tangible costs due to reputation damage.

The study generated a range of estimates to assess the financial impact of website defacement, using a sample of 1,250 defacements reported to the website ‘Zone H’. Zone H is one of the most comprehensive stores of archived website defacements and is an outlet for hackers to publicly report/advertise websites that they have defaced.

The research estimated that the total cost of 1,250 defacements observed between 2007 and 2015 was approximately £1.6 million to the Government and industry targets involved.

Some caution should be exercised when interpreting the estimates from this research. The underpinning cost estimates used were drawn from US Computer Security Institute data, and whilst these were regarded as the best and only available data to use, there are a number of limitations associated with this data set. There are also limitations regarding the information available on the Zone H dataset and it is unclear exactly how representative these cases are of all defacements.

This research importantly highlighted a challenge with estimating costs of cyber crime more generally – a lack of suitable primary data that can be used to develop cost estimates. Further primary research, for example, with businesses, would be required to provide a more accurate UK cost estimate for this and other types of cyber crime.

The study also suggested that there may be value in developing models of the defacement attacks of early, emerging malicious actors – with the idea of identifying which of these actors' activities pose the largest potential for economic loss. This would potentially allow law enforcement, or other mitigation resources, to be assigned using a method of triage to focus attention on the highest priority attacks.

ii. Assessing the scope and cost of malware infections within the UK

The aim of this study, conducted by Dr Tom Holt, was to examine the extent and cost of malware infection using an alternative and lesser used source – the Malware Domain List. The Malware Domain List is an objective, open source that lists malware identified in the wild on web servers hosted in the UK, along with data on the nature of the infection (for example, bots[10], exploit packs[11]).

This study identified 89 total infections observed in the Malware Domain List data between 2009 and 2014. This figure is no doubt an under-representation of the total infections that occurred during this period, but there are no other data sources to validate this. It is unclear why the figure may be so low, possible reasons could be under-reporting to the data source or generally low rates of server-level infections. Thus the findings from this research should be interpreted with extreme caution and it should be considered whether, as a standalone source, the Malware Domain List may not be so valuable for future use.

This study estimates that the identified malware infections may have cost UK-based companies around £5.1 million between 2009–14. While the unit cost figure for malware infections was sourced from a poor quality source, which may affect the level of confidence that can be placed in this estimate, it is important to note that this was one of the only sources available. Should more accurate data sources become available in the future, further primary research, for example, with businesses, could enable the estimation of a more accurate UK cost for this and other types of cyber crime.

iii. Estimating profits and losses to underground markets

This study, conducted by Dr Tom Holt and Dr Olga Smirnova, took an alternative view of the costs of cyber crime by looking at the levels of offender profits.[12] In doing so, the aim of

[10] A tool which executes scripts over the internet.
[11] Software which runs on web servers and identifies weaknesses in client machines communicating with the server.
[12] Offender profits/losses have not been considered by previous Home Office costs of crime research. However, they were considered as part of this work programme in order to explore how an improved understanding of such estimates can

the study was to explore the extent of data and cyber crime services sold in underground online markets, both on the open-web and the ‘dark’ web, that directly target or affect UK citizens, industry or the Government.

The project also aimed to estimate the revenues acquired by underground market actors, such as buyers and sellers of data, and the potential victim costs based on the prevalence of malware, hacking, and personal details that are traded online. It was envisaged that this alternative focus on the costs of cyber crime would complement existing research and help to form a more complete picture of the various costs associated with cyber crime.

Using a sample of 18 forums and 15 shops hosted on the open-web and Tor[13], the study provided a methodology for calculating the number of potential transactions that sellers complete and the potential profits made by data sellers and buyers through these markets.

Based on this sample, the study estimated that sellers offering dumps of credit and debit card data, CVV data (comprising credit card number and Credit Verification Value), and eBay and PayPal accounts may earn anywhere between £4,000 and £16,000 at the minimum price point and between £89,000 and £355,000 at the median price. Within the dark web sample, the study estimated that sellers earned between £13,000 and £54,000 at the minimum price and between £24,000 and £95,000 at the median price. The amounts earned by sellers varied depending on the type, price and quantity of data sold. This creates a substantial variation in profits, but demonstrates that sellers can generate high revenues even at minimum price points and can make the greatest profits through dump sales in particular.

Data buyers' returns were similarly variable. The study estimated earnings to buyers of stolen financial data from samples of transactions from the open web and dark web of between £6.1 million and £25.2 million, depending on how many of the accounts were active if purchased in batches of 50 sets of account data. The study found that buyers have the potential to earn millions of pounds even when controlling for a low probability of useful data or successful transactions. Buyers’ profits are estimated to be in the hundreds of thousands, even when calculating returns with smaller quantities of viable data.

The estimates derived from these models are exploratory, and must be interpreted with caution. They are likely to under-represent the total number of transactions performed and do not account for any labour, time or other unobserved costs on behalf of the seller/buyer. However, the findings demonstrate that selling and buying data are profitable ventures and may account for the longevity of the markets included in this sample of forums

iv. Reputational damage to businesses as a consequence of cyber crime

The aim of this study, conducted by research agency Kantar Public (previously known as

help to progress understanding of the various costs of cyber crime.

[13] A web browser which allows users to access the web (including the darkweb) anonymously.

TNS BMRB), was to conduct primary qualitative research to support the design of a set of quantitative measures that can be replicated and used in future studies to evaluate the impact of cyber crime on business reputation.

The qualitative fieldwork involved depth interviews conducted with a mix of businesses; some of these had experienced cyber crime, and some had not. The businesses included in this initial qualitative work included a mix of small and medium-sized enterprises, and large businesses. Following these depth interviews, a number of focus groups were conducted with members of the public. While the design of this research does not allow the findings to be generalised across the population of the UK, it does allow an insight to be obtained, which is of use to researchers when designing and testing quantitative measures of business reputation.

The research found that both the public and businesses found it difficult to define business reputation in itself, let alone recommend an appropriate measure for assessing change in reputation following a cyberattack. A key finding from the research with businesses was that although participants could imagine proxy measures that might be used to measure the financial impact of reputation damage, they did not imagine that businesses were actively likely to measure the value of business reputation in the absence of a very serious incident. Where such a measurement was to be attempted, the participants explained that this was likely to require the input from multiple separate groups from within their business – in particular IT departments and marketing departments. Furthermore, participants noted that actual calculations would be extremely sensitive and likely to be restricted to boardroom-level conversations. This has implications for how future surveys obtain the necessary information about this kind of impact.

A key finding from the research with members of the public was that cyberattacks did not necessarily result in the public changing companies or providers. There was considerable importance attributed to how businesses handled mistakes or errors. A ‘good’ reputation did not rely on never making mistakes; participants were forgiving about the fact that mistakes happen. However, they expected that where problems occurred, businesses should take responsibility for any errors, swiftly offer solutions and treat customers with respect – they felt that they might be less forgiving of a second attack. These findings suggested some potential practical guidance/considerations for businesses in how best to respond to, or mitigate impacts of, a cyberattack in relation to their business reputation (see Section 7). These could be worth further testing or development.

On completion of the qualitative fieldwork this study considered the development of a set of quantitative measures to evaluate the impact of cyber crime on business reputation. It was clear following discussions with participants of the qualitative research that a single survey measure based on a business’ assessment of the cost of reputation damage is likely to be highly subjective and to provide widely varying estimates. As such, the study concluded that future research should make use of a range of sources from which to triangulate data to give a more comprehensive and robust measure. These sources are likely to include the following.

- **Event studies** – to quantify the cost of reputational damage by using share price as a proxy for reputation.

- **Reputation trackers** – for large consumer-focused firms with high customer numbers, reputation trackers can be used to understand the impact of cyber crime on reputation.
- **Social media analytics** – by forming a set of metrics, analysis can be used to measure the social media response against these metrics.
- **Collecting data from business surveys** – by collecting details about the nature of the attack and the impact on the business, future researchers will be able to identify serious and less serious attacks.

The extent or complexity of the assessment being made might depend on the perceived need of the business. It was thought that at the very minimum, businesses could make some very simple assessments of the likelihood of reputational damage following a cyberattack, based on a number of identified key risk factors identified in the research:

- visibility of the attack amongst customers and key stakeholders;
- direct impacts on customers / stakeholders;
- data security being the primary offer to clients from a business;
- repeat incidents;
- critical timing of the incident; and
- nature of the handling and incident response.

Such assessments could also be used to help develop more considered incident response and handling plans for any future cyberattack.

In response to these conclusions the research team developed a number of suggested survey questions to collect data from future business surveys. These are presented in Appendix 3 of this report.

v. Understanding scale, trends and measurement of cyber-dependent crimes

The aim of this study, conducted by David Emm, Professor Steve Furnell and Dr Maria Papadaki, was to provide a better understanding of the range of measures used to assess the prevalence or incidence of cyber-dependent crimes, including:

- viruses and other malware;
- denial of service or distributed denial of service (DDoS); and
- hacking.

Such measures are used to help compare the extent of the threats that each poses in terms of volumes and frequency. A better preliminary understanding of these measures is helpful when building the evidence base for the costs of cyber crime.

The research involved reviewing various published sources (for example, from security vendors, security surveys and threat reports) to determine the nature and quality of the underlying measures currently (as at 2016) available for cyber-dependent crime.

The review found that variation in current metrics and approaches used means that they do not offer a clear mechanism for quantifying cyber-dependent crime. Current measures can lack depth, comparability and consistency in tracking trends over time. Furthermore the data can be skewed depending on geographic location and because some figures are only based on measures taken from protected devices and reflect only those detected by the vendor.

The study identified that it would be unwise, and potentially misleading, to take a single measure or report in isolation and consider it as the most accurate assessment of scale. Different measures give different levels of insight – they are not ‘wrong’ measures but the choice of metric depends on what exactly is being assessed. A simple measure of volume provides many different, and valid, options.

The review found that there is, however, a clear need to arrive at a more consistent vocabulary, use of terminology and common framework for understanding threats. However, this can add value only if it is promoted widely and strongly enough to ensure widespread adoption and usage. Previous attempts to do this have not succeeded.

The research also considered survey responses from security experts with experience and access to threat data. While the security experts suggested a range of metrics that might be collected to track scale and trends, they were unconvinced about the value of doing so. The general belief was that it is more important to understand the impact of incidents, but that this would pose a different set of challenges for data availability.

The study concluded that measuring the scale, extent and frequency of cyber-dependent crime is not enough on its own. It is also important to relate it at some level to the seriousness, impact and cost of an incident. The big numbers that come out of a global or regional report have a very dramatic effect, but they are not necessarily meaningful for businesses. They need to understand the impact on their business and the actual cost will very much depend upon the impact to the affected organisation.

vi. Exploring the consequences from fear of cyber crime

The aim of this study, by Professor Matthew Williams, was to conduct a European wide comparison of fear of cyber crimes (including economic and content cyber crimes) and avoidance behaviours. Three sweeps of the Eurobarometer Cybersecurity Survey (2012, 2013 and 2014) were combined to facilitate analysis.

Four direct measures of fear of cyber crime were included in the analysis from the Eurobarometer surveys:

- fear of online identity theft;
- fear of online shopping fraud;
- fear of being exposed to indecent images of children; and
- fear of being exposed to material that promoted racial hatred or religious extremism.

These were combined to produce two underlying components:

- fear of economic cyber crime (fear of online identity theft and online shopping fraud); and
- fear of content cyber crime (fear of being exposed to indecent images of children and being exposed to racial or religious cyberhate).

Two questions from the survey were included in the analysis of avoidance behaviour: avoiding online banking and online shopping.

Overall, the study found that the burden of fear is greater for economic cyber crime than for content cyber crime. Great Britain (GB) was placed sixth most fearful of economic cyber crime in Europe, after the Czech Republic, Lithuania, Spain, Latvia and France. Ireland emerged as seventh most fearful of economic cyber crime. Interestingly a group of Nordic countries in the EU (Sweden, Denmark and Finland) and the Netherlands occupied the lower end of the plot, exhibiting the least fear of economic cyber crime, along with Romania, Hungary and Slovenia.

Furthermore, the study found that GB was placed fourth most fearful of content cyber crime in Europe, after the Czech Republic, Spain and Lithuania. Ireland and France emerged as sixth and seventh most fearful of content cyber crime. As with economic cyber crime, a group of Nordic countries (Sweden, Denmark and Finland) and the Netherlands occupied the lower end of the plot, exhibiting the least fear of content cyber crime.

GB was placed fifth in terms of online avoidance adoption, after Sweden, Luxembourg, Belgium and the Netherlands. France and Ireland emerged as sixth and ninth in terms of avoidance adoption. Eastern European countries (Bulgaria, Latvia, Poland, Slovakia, Lithuania and Estonia) exhibited the least avoidance adoption.

Multi-level regression analysis showed experiencing content cyber crime was the strongest predictor of online avoidance adoption, while experience of economic cyber crime emerged as third most predictive. Women, the elderly, and the economically disadvantaged were all statistically significantly more likely to adopt avoidance behaviours. Victims of cyber crime, women, parents, the economically disadvantaged and those living in rural locations were statistically significantly more likely to fear cyber crime. Age was also significantly predictive of fearing cyber crime. In Europe fear peaked at age 38 for economic cyber crime (45 for men and 31 for women) and age 43 for content cyber crime (47 for men and 37 for women). In GB fear of economic cyber crime in peaked at 46 years and fear of content cyber crime peaked at 47 years.

The study concluded by considering how estimating the monetary costs of cyber crime is desirable for policymakers and the judiciary. The study noted that while some methods, such as shadow pricing (a pricing exercise using proxy values determined by the likely opportunity cost to obtain a good or commodity) have been applied to fear of offline crime, the same methods cannot be applied to cyber crime as the data are currently not available. However, it may be possible to perform monetary cost estimations in the near future in relation to both individual and business cyber crime once data sets become available (e.g. the CSEW).

5. Discussion and directions for future research

This report has highlighted a number of key insights that build on the extant literature and help to raise awareness of key considerations when estimating costs associated with cyber crime. Examples of new cost estimates include the following.

- A study estimated that the total cost of 1,250 web defacements, observed between 2007 and 2015, was £1.6 million to the Government and industry targets, with a cost per defacement of approximately £1,200.[14]
- A study focusing on malware infections reported at the server level within the UK, found that the estimated cost to UK-based companies of 89 malware infections reported to the Malware Domain List between 2009 and 2014 was £5.1 million, with an average cost per infection in excess of £57,000.[15]
- Research based on a sample of transactions within a period found that buyers of stolen financial data from the open web and dark web are estimated to earn between £6.1 million and £25.2 million from the use of that data, depending on how many of the accounts were active if purchased in batches of 50 sets of account data.
- Research exploring earnings to sellers of stolen financial data resulted in a new median estimate of between £89,000 and £355,000. Within a dark web sample, sellers earned between £24,000 and £95,000 at the median price.

It is important to note that these findings still have limitations. They are often based on small samples of available data and are likely to be only a small element of the likely total costs. They are also reliant on the quality of the underpinning data sources - the studies found that there was a distinct lack of high quality primary data available for unit cost estimates. This meant studies were reliant on the few sources available, which were known to have a variety of limitations.

However, these findings have still helped to explore and understand the value of alternative data sources for further knowledge in this area. One study also provides an alternative view of looking at costs – from an offender perspective.

In addition to providing new understanding of some of the costs associated with cyber

[14] Although it is important to note that cost is variable from year to year, so this is not a static figure.

[15] Although it is important to note that the malware type affects individual costs and costs vary by year, meaning that exact costs per infection may differ from this average value.

crime, qualitative research undertaken as part of the project investigating ways of measuring the impact of cyber crime on business reputation, identified a number of possible approaches businesses could take to gain a better sense of the impacts of a cyberattack on their reputation (as outlined in Section 6). The same research also identified that members of the public attribute a sense of importance to how businesses handle mistakes or errors. Participants discussed how they were forgiving about the fact that mistakes happen, but that they expected where problems occurred, businesses should take responsibility for any errors, swiftly offer solutions and treat customers with respect – they felt that they might be less forgiving of a second attack. These types of findings could be used by businesses to help inform their response to consumers / clients. Key aspects of a good quality post-incident response were felt by consumers and businesses interviewed, to include:

- a swift, honest and informed response;
- communications to customers coming directly from the company (not second hand, via the media);
- good quality customer service in response to queries following the incident, e.g. customer service staff should provide consistent and knowledgeable advice about the incident, should be reassuring and responsive to customer queries; and
- provision of reimbursement or compensation for losses and / or inconvenience where necessary.

Given how important the handling and incident response was regarded by interviewees – it was notable that the businesses interviewed had not generated incident response plans for such an attack. Rather than simply looking to ‘weather the storm’ it appeared that businesses could take more action to help prepare themselves in the event of an attack.

Overall, the work programme has been instrumental in gaining a better understanding of how researchers might, in future, go about estimating an overall cost of cyber crime or estimating the various different aspects of cyber crime. While this report does not attempt to arrive at an overall estimate of the cost of cyber crime, the development of the costs of cyber crime framework (see Table 2) helps to take the research community closer towards achieving that goal. The framework is intended to provide researchers with a clearer sense of direction when designing future research studies to fill the numerous research gaps in a consistent fashion.

The literature review, undertaken as part of the work programme, identified a range of challenges and limitations with the costs estimates available during the time of the research programme. A particular limitation was that many studies were dependent on poor quality survey data on the scale and costs of cyber crime, which were used to underpin their estimates. Although this dependency on poor quality data has impacted previous research work, going forward there is much to be optimistic about in terms of new survey and data developments that can help to improve future estimates.

In 2016 the Department for Culture Media and Sport published the findings of its new survey of businesses – the Cyber Security Breaches Survey (DCMS, 2016).[16] This survey presented a range of useful findings, including the £36,500 estimated average cost of a breach to large businesses and the £3 million estimated most costly breach identified in the survey. This survey is a refreshed version of a survey conducted in previous years by the Department for Business, Innovation and Skills (BIS) and private sector business Price Waterhouse Cooper, and now represents the most robust methodological approach used by the survey to date. The method used by the survey was a random probability telephone survey of 1,008 UK businesses, with the data weighted to be statistically representative of the population of UK businesses based on size and sector. The findings of this survey present a valuable opportunity to researchers to gain a better understanding of the effects of cyber breaches in the UK, and going forward should enable the identification of cyber breach trends, allowing researchers to understand how such activity changes over time.

Similarly, work has been conducted to improve estimates of the prevalence of cyber crime, following a field trial of new questions to be included in the Crime Survey for England and Wales by the Office for National Statistics (ONS, 2015). Following the addition of new questions in the survey, ONS (2017) published experimental data showing that there were an estimated 3.6 million fraud and 2.0 million computer misuse offences experienced in England and Wales in the year ending September 2016.[17] The experimental data showed that 61 per cent of total fraud offences involved financial loss and of those offences that involved financial loss, 23 per cent were losses greater than £500. Unfortunately these data were not available during the course of the Working Group, so could not be used. Early analysis of data captured through the inclusion of these questions however, offers a greater understanding of the extent of cyber crime (*ibid.*) and is likely to be of much use to law enforcement agencies and policymakers going forwards, as they work to ensure the optimal allocation of resources to tackle cyber crime.

Other recent surveys also offer an opportunity for further exploration. For example, the Home Office Commercial Victimisation Survey (CVS), continues to generate useful data on cyber crime for specific sectors, at a premises level. Bossler, Holt and Burruss' (2016) survey of UK police forces investigated the views and cyber crime policing experiences of UK police community support officers, constables and sergeants. Questions were asked in this survey about the time spent dealing with various cyber crimes and could be used to conduct further exploratory work regarding law enforcement costs for dealing with cyber crime – currently a big evidence gap in the framework.

[16] The most recent version to date of this survey was published in April 2017, and can be found here: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017

[17] The most recent ONS experimental data was published in October 2017 and can be found here: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017

Where surveys are able to offer robust methodological approaches, i.e. incorporating random probability sampling methods, and are able to help to fill key gaps in a consistent fashion as identified in the costs of cyber crime framework, then there is potential for developing understanding in this area. It is, however, vital that those attempting to estimate costs consider how the survey samples being used have been selected, and whether they are truly representative of the wider population of interest.

However, aside from survey developments, there are various other opportunities for furthering the evidence base regarding costs of cyber crime. As such, this report concludes by making a number of recommendations to inform the design of future research.

- **Researchers designing future costs of cyber crime studies should: approach their research design in a systematic fashion using the framework in this report; identify gaps in the costs of cyber crime framework; and tailor research questions so that they can fill these specific gaps.** To enable comparability of results, researchers should focus on investigating the economic cost of cyber crime to the UK per incident, and arriving at a separate estimate for the volume of incidents per year. The cost per incident estimates can then be multiplied by the separate prevalence estimates and the resultant totals summed. In the longer term this will take the wider research community further towards understanding the total cost of cyber crime.

- **Future research should focus on the most notable gaps in the costs of cyber crime framework.** For example, the literature review did not identify any component costs for hacking/computer intrusions; nor had previous research considered law enforcement response costs. Law enforcement costs notably represent an important gap and priority area for research, given the challenges that may be faced by law enforcement in deterring and pursing offenders in an online environment. Similarly, previous research has focused disproportionately on the costs incurred by businesses and on cyber-enabled crime (particularly fraud). Future studies should further consider the costs of cyber crime incurred by individuals and consider the full range of cyber crimes, including cyber-dependent crimes. Focusing new studies on these identified gaps, as well as improving upon estimates already made, would be useful in increasing the overall level of knowledge around the costs of cyber crime.

- **Future studies should further investigate the costs and profits to offenders of engaging in cyber crime.** Study findings presented in this report indicate that research into this particular cost area could be of much use to policy makers. This is likely to be of particular relevance in the context of the new *National Cyber Security Strategy* (HM Government, 2016) which emphasises the importance of raising the costs and reducing the rewards for cybercriminals, and taking steps to increase the barriers to entry for cyber crime. Future research in this area should seek to understand these costs in greater detail and consider how the impacts of any future interventions may best be evaluated.

- **Future studies should seek to test the measures presented in Appendix 3 of this report by investigating the financial impact of cyberattacks on the**

value of business reputation. It is important to note that the primary research conducted to develop the trial measures recommended that any surveys on which they are included would need to be completed by multiple representatives from responding businesses, in order to obtain accurate and reliable results.

- **Further analysis of the Action Fraud data set should be conducted to make best use of the available cost data.** Whilst the report conducted for City of London Police went some way to analyse the available data, there is more use to be made of this data set as the data quality and reporting improves.

- **Future research should further consider how to estimate the monetary cost of the fear of cyber crime.** Once new data become available to researchers the shadow costing method should be applied to fear of cyber crime amongst the domestic population to estimate financial costs.

- **Future studies should explore the use of increasingly robust survey data when estimating the costs of cyber crime. For example, the CSEW measure of cyber crime and DCMS Cyber Security Breaches Survey.** Applying these increasingly robust data to the costs of cyber crime framework presented in this report should enable researchers to produce consistent and robust cost estimates which make best use of available information.

References

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. (2012) *Measuring the cost of cyber crime*. Available at: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf Last accessed: 1st December 2016.

Bossler, A.M., Holt, T.J. and Burruss, G (2016) *Examining UK constables' perceptions of cyber crime.* Presentation at the annual meeting of the American Society of Criminology, New Orleans, LA.

British Retail Consortium (2015) *BRC Retail Crime Survey 2014*. Available at: http://www.soloprotect.com/uk/Data/Lone_Downloads/BRCRetailCrimeSurvey2014.pdf Last accessed: 1st December 2016.

Centre for Economics and Business Research (2015) *The business and economic consequences of inadequate cybersecurity*. Research report prepared for Veracode. Available at: https://info.veracode.com/analyst-report-cebr-business-and-economic-consequences-of-inadequate-cybersecurity.html Last accessed: 1st December 2016.

Cifas (2014) *Fraudscape: UK fraud trends*. Available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/External%20-%20Fraudscape%20main%20report%20for%20website.pdf Last accessed: 1st December 2016.

City of London Police (2015) *The implications of economic cyber crime for policing*. Available at: https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf Last accessed: 1st December 2016.

DCMS (2016) *Cyber Security Breaches Survey. Main Report.* London: Department for Culture Media and Sport. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf Last accessed: 1st December 2016.

Detica (2011) *The cost of cyber crime.* Available at: *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf* Last accessed: 1st December 2016.

Financial Fraud Action UK (2015) *Fraud the Facts 2015. The definitive overview of payment industry fraud and measures to prevent it.*

Florencio, D. and Herley, C. (2011) 'Sex, lies, and cyber-crime surveys'. In *Proceedings (online) of the Workshop on Economics of Information Security.* Microsoft Research. Available at: http://research.microsoft.com/pubs/149886/SexliesandCyber crimeSurveys.pdf Last accessed: 1st December 2016.

Gee, J. and Button, M. (2015) *Countering fraud for competitive advantage: How UK FTSE listed companies can reduce the cost of fraud and maximize profitability.* PFK Littlejohn LLP. Available at: https://www.accountant.nl/contentassets/40dd3944bac9446f9bf8162f3fec650a/countering_fraud_for_competitive_advantage_2015.pdf Last accessed: 1st December 2016.

Government Statistical Service (2011) *National Statistician's Review of Crime Statistics: England and Wales, June 2011*. Available at: https://www.statisticsauthority.gov.uk/archive/national-statistician/ns-reports--reviews-and-guidance/national-statistician-s-reports/national-statistician-s-review-of-crime-statistics.pdf Last accessed: 1st December 2016.

HM Government (2015) *2015 Information Security Breaches Survey.* Available at: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf Last accessed: 1st December 2016.

HM Government (2016) *National Cyber Security Strategy 2016–2021.* Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf Last accessed: 1st December 2016.

HM Treasury (2003[18]) *The Green Book. Appraisal and Evaluation in Central Government*. Available at: https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-governent Last accessed: 1st December 2016.

Home Affairs Select Committee (2013) *House of Commons Home Affairs Select Committee Report on E-crime*. Available at: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf Last accessed: 1st December 2016.

Home Office (2000) *The economic and social costs of crime*. London: Home Office. Available at: http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/pdfs/hors217.pdf Last accessed: 1st December 2016.

[18] Revised in 2011.

Home Office (2013a) *Serious and Organised Crime Strategy.* London: Home Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf Last accessed: 1st December 2016.

Home Office (2013b) *Understanding organised crime: estimating the scale and the social and economic costs*. London: Home Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246390/horr73.pdf Last accessed: 1st December 2016.

Home Office (2013c) *Cyber Crime: A Review of the Evidence.* London: Home Office. Available at: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence Last accessed: 1st December 2016.

Intellectual Property Office (2015) *IP Crime Report 2014/2015.* Available at: https://www.gov.uk/government/publications/annual-ip-crime-report-2014-to-2015 Last accessed: 1st December 2016.

McAfee/Intel (2014) *Net losses: Estimating the global cost of cyber crime. Economic impact of cyber crime II*. Center for Strategic and International Studies. Available at: http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf Last accessed: 1st December 2016.

National Crime Agency (2015) *National Strategic Assessment of Serious and Organized Crime 2015.* Available at: http://www.nationalcrimeagency.gov.uk/publications/560-national-strategic-assessment-of-serious-and-organised-crime-2015/file Last accessed: 1st December 2016.

National Fraud Authority (2013) *Annual Fraud Indicator.* Available at: https://www.gov.uk/government/publications/annual-fraud-indicator--2 Last accessed: 1st December 2016.

Neustar (2015) *Neustar DDoS Attacks & Protection Report: EMEA* (Europe, the Middle East and Africa), March 2015*.* Available at: https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2015-uk-ddos-report.pdf Last accessed: 1st December 2016.

ONS (2015) *CSEW Fraud and Cyber-crime Development: Field Trial"*. Available at: http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/methodological-notes/methodological-note---csew-fraud-and-cyber-crime-development--field-trial---october-2015.pdf Last accessed: 1st December 2016.

ONS (2017) *Crime in England and Wales: Year ending Sept 2016*. Available at: https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingsept2016 Last accessed: 8th March 2017.

Oxford Economics (2014) *Cyber-Attacks: Effects on UK Companies.* A Report for the Centre for the Protection of National Infrastructure.

Ponemon Institute (2015) *2015 Cost of Cyber Crime Study: United Kingdom*. *Benchmark Study of UK Companies.* Last accessed: 1st December 2016: http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/index.html

Ponemon Institute (2016) *Flipping the Economics of Attacks.* Available at: http://www.ponemon.org/library/flipping-the-economics-of-attacks Last accessed: 1st December 2016.

Symantec (2013) *2013 Norton Report – UK.* Available at: http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.en_uk.pdf Last accessed: 1st December 2016.

Symantec (2015) *ISTR 20* (Internet Security Report Threat).

ThreatMetrix (2015) *ThreatMetrix cyber crime report Q3.* Available at: https://www.threatmetrix.com/wp-content/uploads/2015/11/ThreatMetrix-Cybercrime-Report-Q3-2015.pdf Last accessed: 1st December 2016.

Verizon (2015) *2015 Data Breach Investigations Report.* Available at: http://www.verizonenterprise.com/DBIR/2015/ Last accessed: 1st December 2016.

Wall, D. S. (2007[19]) 'Policing cyber crimes: Situating the public police in networks of security within cyberspace', *Police Practice & Research: An International Journal*, 8 (2), pp 183–205.

World Economic Forum (2014) *Global Information Technology Report 2014: Rewards and Risks of Big Data.* Available at: http://www.weforum.org/reports/global-information-technology-report-2014 Last accessed: 1st December 2016.

[19] Revised in May 2010 and February 2011.

Appendices

Appendix 1 provides a more detailed literature review on the costs of cyber crime.

Appendix 2 provides a glossary of the terms used in the costs of cyber crime framework.

Appendix 3 provides draft quantitative measures designed to quantify the value of business reputation, in order to evaluate the impact of cyberattacks on business reputation.

Appendix 4 provides information on where to find more detailed published work on some of the studies discussed in this report that were commissioned by the Costs of Cyber Crime Working Group.

Appendix 5 outlines the Costs of Cyber Crime Working Group’s Terms of Reference.

Appendix 6 provides a list of members of the Costs of Cyber Crime Working Group.

Appendix 1: More detailed literature review on the costs of cyber crime

In order to understand the wide range of cost estimates reported in previous research findings, a literature review was conducted using an online search for UK cyber crime cost estimates that were published before 1 January 2016 dating back to the Detica (2011) report. The literature review was conducted by Dr Adam Bossler, with support from Home Office Analysis and Insight.

Detica, 2011

Taking the Detica (2011) paper as a starting point, it is important to note that the definition of cyber crime used in that paper (*"the illegal activities undertaken by criminals for financial gain, which exploit vulnerabilities in the use of the Internet and other electronic systems to illicitly access or attack information and services used by citizens, business and government"*) differs from the definitions used in this research and in other similar studies, which break cyber crimes down into cyber-enabled and cyber-dependent crimes. This highlights one of the key issues identified by this literature review – that definitions used and applied by researchers working in the field are inconsistent to the point that it is often not possible to compare and contrast reported estimates. This does not just apply to the definition of 'cyber crime', but also to the definitions of various other concepts that affect the overall costs of cyber crime.

Taking into consideration the definition of cyber crime used in the Detica paper, this meant a focus on:

- identity theft and online scams;
- intellectual property (IP) theft, espionage and extortion; and
- fiscal fraud against the Government.

The study involved the development of a causal model, linking cyber crimes to their impact on the UK economy. The Detica paper adapted the Home Office (2000) approach to estimating the cost of crime, so that it included:

- costs in anticipation;
- costs as a consequence;
- costs in response; and
- indirect costs associated with cyber crime (for example, reputation damage, loss of confidence).

The Detica paper particularly focused on costs as a consequence with some additional costs in response included. Costs in anticipation of cyber crime were not considered in detail. The model was then used to map cyber crime types to categories of economic impact. This meant that the model could be used to calculate the magnitude of the costs of cyber crime using three-point estimates – worst-case, most likely case and best-case scenarios – although it is important to note that not all three types of estimate were always presented in the report.[20] The report concluded that in the most likely scenario, the estimated cost of cyber crime to the UK was £27 billion, with the authors noting that this was likely to be an underestimate.

The overall £27 billion cost estimate was derived from a number of other cost estimates presented in the report, key examples of which are contained in the following tables.

Example costs from the Detica (2011) report:

Costs to citizens	
Cyber crime	**Economic impact**
Identity theft	£1.7bn
Online fraud	£1.4bn
Screenware and fake AV	£30m

1 AV is antivirus.

Table A1.1: Estimates of costs to citizens of cyber crime in the UK
Source: Detica (2011)

Costs to the Government	
Cyber crime	**Economic impact**
Fiscal fraud	£2.2bn

Table A1.2: Estimates of costs to the Government of cyber crime in the UK
Source: Detica (2011)

Costs to businesses	
Cyber crime	**Economic impact**
IP theft – Aerospace and defence	£0.4bn
IP theft – Chemicals	£1.3bn
IP theft – Electronic and electrical equipment	£1.7bn
IP theft – Software and computer services	£1.6bn
IP theft – Healthcare, pharmaceutical and biotechnology	£1.8bn

[20] For example, for customer data loss only best-case and worst-case estimates were presented in the report.

Industrial espionage – Aerospace and defence	£1.2bn
Industrial espionage – Financial services	£2.0bn
Industrial espionage– Mining	£1.6bn
Customer data loss (best case)	£0.96bn
Online theft from business (most likely case)	£1.3bn
Extortion (most likely case)	£2.2bn

Table A1.3: Estimates of costs to businesses of cyber crime in the UK
Source: Detica (2011)

This Detica estimate was based on a snapshot of costs from 2010, substituting for the best available alternative source of data where 2010 data were not available, treating these alternatives as if they were 2010 data.

It is important to note that there were a number of limitations associated with the Detica cost estimates. Many of these limitations relate to assumptions made by the report authors, which played a crucial part in arriving at the reported cost estimates. Example assumptions include:

- that only 1 in 15 incidents are reported by citizens;
- 25 per cent of identity fraud crimes are committed online;
- all criminal attacks from the National Fraud Authority (NFA) Annual Fraud Indicator were cyberattacks.

The accuracy of these assumptions is likely to be of considerable importance when evaluating the level of confidence that can be attributed to the cost estimates reported. Furthermore, a number of assumptions were made for which full details were not provided, for example:

- the revenue impact on the company if a rival is able to exploit stolen IP (assumed revenue impact not specified);
- the proportion of a sector's value-added to the UK economy that is dependent on large-scale tendering competitions (proportion not specified);
- probability that a sector's value-added would be subject to cyberattacks (probability not specified).

The lack of transparency associated with the derivation and use of such assumptions creates further limitations to the degree of confidence that can be attributed to the cost estimates reported.

In addition to the issues with the transparency of assumptions and calculations used in the research, a number of methodological decisions were taken in the Detica research that could affect the reliability of results. For example, the decision not to consider costs associated with IP-rich firms increasing their cyber-protection (as the authors considered these costs to be business-as-usual) and the decision to exclude costs borne by individuals in anticipation of cyber crime (firewall, anti-virus software, etc.). Such considerations reinforce concerns with the reliability of the overall £27 billion cost estimate, as well as the various lower level estimates that contributed to this total.

Anderson, Barton, Bohme, Clayton, van Eeten, Levi, Moore and Savage, 2012
Anderson *et al*. (2012) published their report, *Measuring the cost of cyber crime,* in response to concerns with previous reports, notably the Detica (2011) report, which it was believed may have overestimated the costs of cyber crime. The report adheres to the following definitions of cyber crime, which were proposed by a European Commission communication in 2007.

- Traditional forms of crime such as fraud or forgery, committed over electronic communication networks and information systems.
- The publication of illegal content over electronic media (for example, child sexual abuse material or incitement to racial hatred).
- Crimes unique to electronic networks, for example, attacks against information systems, denial of service and hacking.

To analyse the costs of cyber crime, based on this definition, the report authors estimated global figures. In doing so, the authors worked on the assumption that the UK accounted for approximately 5 per cent of world gross domestic product (GDP) to enable national estimates to be scaled up or down. The authors noted that where this approach was not suitable they would say so in the report and make *"an appropriate allowance".*
The report authors considered the approach taken in the Detica (2011) paper:[21]

- the estimation of costs in anticipation of cyber crime;
- costs as a consequence of cyber crime;
- costs in response to cyber crime; and
- indirect costs such as reputational damage.

The authors expressed concern with this methodology as the 'costs as a consequence' heading includes both direct and indirect costs; the authors claiming that indirect costs are harder to assess accurately than direct costs. Furthermore, the authors felt that costs in response to cyber crime were made up entirely of direct costs. In response to these concerns, Anderson *et al*. proposed an approach, which they considered to be more straightforward, in which they split direct costs from indirect costs. Costs of security and social and opportunity costs of reduced trust in online transactions were also covered. In applying the framework, the report uses the following definitions.

- Direct losses: The monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of cyber crime.
- Indirect losses: The monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cyber crime is carried out, no matter whether successful or not and independent of a specific instance of that cyber crime.
- Defence costs: The monetary equivalent of prevention efforts.

The costs used in the analysis were taken from various research and statistical sources within the available literature, and where necessary assumptions were made by the report

[21] And the Home Office Economic and Social Costs of Crime report (2000).

authors to arrive at the costs provided in the report's summary table. An extract of the summary table is provided here as an example (Table A1.4).

Type of cyber crime	UK estimate	Global estimate	Reference period
Cost of genuine cyber crime			
Online banking fraud			
- Phishing	$16m	$320m	2007
- Malware (consumer)	$4m	$70m	2010
- Malware (business)	$6m	$300m	
- Bank tech countermeasures	$50m	$1,000m	2010
Fake antivirus	$5m	**$97m**	2008-10
Copyright-infringing software	**$1m**	**$22m**	2010
Copyright-infringing music etc.	$7m	**$150m**	2011
Patent-infringing pharma	**$14m**	**$288m**	2010
Stranded traveller scam	$1m	**$10m**	2011
Fake escrow scam	$10m	**$200m**	2011
Advance-fee fraud	**$50m**	$1,000m	2011
Costs of transitional crime			
Online payment card fraud	**$210m**	$4,200m	2010
Offline payment card fraud			
- Domestic	$106m	$2,100m	2010
- International	$147m	$2,940m	2010
- Bank / merchant defence costs	$120m	$2,400m	2010
Indirect costs of payment fraud			
- Loss of confidence (consumers)	**$700m**	**$10,000m**	**2010**
- Loss of confidence (merchants)	**$1,600m**	**$20,000m**	**2009**
PABX fraud	**$185m**	**$4,960m**	2011

*Figures in bold are estimates based on data or assumption for the reference area. Unless both figures are involved, the non-bold figure has been scaled using the UK's share of world GDP, unless otherwise stated.

Table A1.4: Costs of Cyber Crime estimates by Anderson et al (2012)
Source: Anderson et al. (2012)

Within this summary table, crimes were only recorded that imposed annual worldwide costs in excess of $10 million. Bold highlighting is used within the table to indicate that non-bold highlighted values have been scaled based on the UK's share of world GDP.

It is difficult to evaluate the reliability of a number of the values reported in Table A1.4. In part, this is because of the dependence on the work of others to arrive at component values used within the analysis. Additionally, within the Anderson *et al*. paper a number of assumptions are made for which the reasoning is not entirely clear. As an example, consider the following extract that relates to the estimated cost of patching software.

"The part of this cost that can be attributed to the UK will probably be at most its share in global GDP, as its software industry is proportionally smaller than that in the USA. If we assume, for illustrative purposes, that the global cost of patching is $1 billion per year, this would mean the UK bears $50 million of this. This does not include the costs of deployment, which are borne by the end users." (Anderson *et al*., 2012, p 22)

Based on this extract of the report, there is no indication of where the $1 billion cost to the global economy originated from and as such, it is difficult to evaluate the robustness of this $50 million cost estimate.

Furthermore, there are limitations of the reliance of this approach on use of GDP, as *'depending heavily on a GDP-based share of total crime costs to calculate UK estimates relies both on the accuracy of the global estimates used and the assumption that the relative proportion of an offending category in the UK is always equal in cost to its proportionate GDP'* (Home Office, 2013c).

It should be noted that the Anderson *et al*. report does not include figures for industrial cyber-espionage and extortion as *"there is no reliable evidence of the extent or cost of industrial cyber-espionage and extortion"* (p 18). Considering, however, that this estimate comprised a large proportion (£2.2 billion) of Detica's (2011) overall cyber crime cost estimate, the exclusion of cyber-espionage and extortion estimates in the Anderson *et al*. report partially explains the considerable difference in overall estimates. Although Anderson *et al*. state that Detica's estimates may not have *"obvious foundations"*, numerous news reports of foreign nations hacking into the computer networks of governments and corporations, presumably to steal proprietary information among other things, makes it likely that any estimate not including the costs associated with the stealing of intellectual property and commercially sensitive information may grossly underestimate the cost of cyber crime.

Oxford Economics, 2014

The Oxford Economics study on the effects of cyberattacks on UK companies was published following a request from the Centre for the Protection of National Infrastructure (CPNI) to investigate the impact of state-sponsored cyberattacks on UK firms. In addition to producing an economic framework to understand these impacts, the study also consisted of:

- a survey of UK firms to estimate the cost impact of cyberattacks;
- an event study investigating the impact on market valuations of cyberattacks; and
- a number of case studies illustrating UK firms' experiences of cyberattacks.

Within the report the authors briefly discuss typologies for considering the costs of cyber crime and adopt the Home Office (2000) model:

- costs in anticipation;
- costs as a consequence; and
- costs in response.

The survey results presented in the report were based on an email/internet-based questionnaire sent to a database of IT professionals, IT security practitioners and other IT-related roles. This database was selected for the sample as a matter of convenience as it had been used in previous similar surveys by the Ponemon Institute – the sub-contractor responsible for the survey work. In total, 9,973 surveys were issued and following screening, a response of 427 was achieved – a response rate of 4.3 per cent, which the authors comment was above the mean average for that industry. Given the sampling approach used, the survey results presented in this paper cannot be considered representative of the population of UK firms.

The survey results reported that 60 per cent of respondents had experienced a cyberattack within the past 12 months, with 31 per cent of those who experienced a cyberattack reporting that they had lost sensitive information. As was the case with other results presented from the survey questions, the authors did not provide information on how many non-responses were received to this question. It is also important to note that to answer this question affirmatively requires the business to be aware that it has suffered from a cyberattack and for the person answering the questionnaire to have been informed of that cyberattack – as such, the true proportion of businesses that experienced a cyberattack during the previous 12 months may have been greater than the reported 60 per cent.

The survey results also reported a number of loss estimates as a result of cyberattacks.

Item	Clean-up / remediation (n=375)	Lost productivity (n=375)	Disrupted operations (n=375)	Damage / theft of IT (n=371)	Reputation / Branding (n=272)
Mean	2.3	1.9	2.3	1.9	2.9
Adjusted mean	0.8	0.9	0.8	0.8	0.9
Median	0.18	0.18	0.18	0.18	0.38

Table A1.5: UK firm cyberattack costs over 24 months (£ million)
Source: Oxford Economics (2014)

The authors noted that critics of previous studies had questioned the usefulness of means reported from such surveys due to the robustness issues created by large outliers and small sample sizes. The authors responded to these criticisms by highlighting that the purpose of their research was not to extrapolate over the entire population of UK businesses, rather to highlight the results from the sample of businesses surveyed (Oxford Economics, 2014, p 3). They had taken steps to adjust the mean (in the table above) by excluding outliers – observations more than 2.5 standards from the mean – and reporting a median value alongside the mean and adjusted mean values.

The survey results also reported intellectual property and commercially sensitive information loss estimates as a result of cyberattacks (Table A1.6).

Item	IP costs (n=69)	Commercially sensitive business costs (n=69)
Mean	17.3	15.1
Adjusted Mean	13.2	12.8
Median	7.5	7.5

Table A1.6: UK firm losses of intellectual property and commercially sensitive business costs due to cyberattacks over the previous 24 months
Source: Oxford Economics (2014)

When presenting these results the authors note that it is important to consider that 80 per cent of respondents indicated that they had not experienced any intellectual property or commercially sensitive information loss in the previous 24 months. The authors conclude that the reported results of the survey are not generalisable, but they might suggest that while only a minority of businesses suffer such losses the cost of such losses are higher than other costs arising as a result of a cyberattack.

In addition to the survey results reported above the report also detailed an event study to analyse the potential reputational loss that firms may suffer along with a number of case studies of firms that had experienced a cyberattack, considering how these attacks had affected their operations. As a proxy for reputational damage the authors used negative stock market returns, which may be experienced immediately around the public disclosure of a cyberattack. By investigating average abnormal returns the authors found that average abnormal returns for more than half of the events were negative, indicating a negative stock market valuation as a result of a cyberattack. However, statistically significant results were only found for three such firms. For these firms, it may be the case that they experienced reputational loss in addition to other costs arising from the cyberattacks that they experienced.

Ponemon Institute, 2015

The Ponemon Institute’s (2015) annual study of UK companies regarding the costs of cyber crime examined the total costs that organisations suffer because of cyberattacks, including:

- detection, investigation and escalation;
- containment;
- recovery;
- ex post response;
- efforts to reduce the impact of the attack on information loss or theft, business disruption and equipment damage; and
- revenue loss.

The authors defined ‘cyberattack’ as: *“Criminal activity conducted via the Internet. These attacks can include stealing an organization’s intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country’s critical national infrastructure”* (Ponemon Institute, 2015, p 1).

Their methodology consisted of conducting 326 interviews of personnel in 39 large-sized organisations. As the authors state in the report, *“each annual study involves a different sample of companies. In other words, we are not tracking the same sample of organisations over time”* (p 2). Therefore, differences in estimates from year to year may be differences in the organisations sampled rather than actual changes in costs.

The Ponemon Institute found that in 2015, the average annualised cost for the 39 corporations was £4.1 million per year (median of £3.4 million), a 14 per cent increase from 2014, with a range between £628,423 to £16 million. These costs were estimated by asking the personnel to report the costs of cyberattacks over a four-week period, which was then utilised to create an annual estimate. It is unclear from the report whether this was a recent specified four-week period or a typical four-week period. The costs, however, differed substantially depending on the industry segment examined. For example, in 2015 financial, energy and utilities, and communications organisations experienced higher cyber crime costs than organisations in retail, the public sector, and education and research. In addition, the research found that organisational size is positively correlated to annualised cyber crime cost. The Ponemon Institute (2015) also estimated that business disruption costs and revenue losses were the top two external costs while recovery and detection were the most costly internal activities.

The Ponemon Institute (2015) provides some limitations of its methodologies. These should be taken into consideration when examining its estimates and they decrease the ability to generalise from the results. Some of the limitations include that the Ponemon Institute (2015), similar to other companies, used its own confidential and proprietary benchmark method, which does not allow for outside scrutiny. In addition, its methodology consists of:

- a sampling plan that does not allow for statistical inferences;
- issues with non-response bias;
- a sampling frame bias in that it believed that it sampled companies with more mature information security programs; and
- reliance on the integrity of the respondents in providing the responses.

Centre for Economics and Business Research, 2015

The Centre for Economics and Business Research’s (Cebr’s) 2015 report provides information on how 201 C-suite executives (a colloquial term used to describe executives in senior management who tend to have the word ‘chief’ in their titles) viewed cybersecurity and the costs associated with cyberattacks. It reports that: *“the survey, and data collected from the Annual Business Survey (ABS), allowed Cebr to estimate the number of businesses that were affected by cyber crime. Cebr also estimated the revenue lost due to cyber crime in the UK and the extent of the increase to IT spending in order to react to a cybersecurity breach”* (p 22).

Cebr found that 15 per cent of the UK firms reported having a security breach in which they lost revenue. The top concerns of the respondents regarding cyberattacks were the breach costs, including but not limited to:

- forensics;
- clean-up;
- legal;
- the reputation and brand damage that results from losing customer data; and
- the lost revenue due to downtime.

Cebr estimated that cyberattacks caused a loss of £18 billion in revenue for UK firms as a result of the cyberattacks. In addition, they spent almost £16 billion in subsequent increased IT spending. Almost all the firms (88%) reported that they increased their annual IT spending in order to address breaches. A majority of chief technology officers – 70 per cent – believed that their current cybersecurity policies actually blocked innovation, indicating an indirect cost of increasing security. The report also found that theft of intellectual property ranked as the sixth highest priority among the respondents although one-third of cyber crime was tied to intellectual property theft for UK businesses.
It was not clear how the sample of 201 C-suit executives was selected, how representative the sample was of the wider population or how many of those approached responded to the survey. As such, it is not clear how generalisable these findings are.

Examples of reports on fraud estimates

Financial Fraud Action UK, 2015

Financial Fraud Action UK (FFA UK) *"is responsible for leading the collective fight against fraud in the UK payments industry"* and its *"membership includes banks, credit, debit and charge card issuers, and card payment acquirers in the UK"* (Financial Fraud Action UK, 2015, p 2). In its report, FFA UK estimated that fraud losses on UK-issued cards totalled £479 million in 2014, a 6 per cent increase from the previous year; £217.4 million of this total was e-commerce fraud and £60.4 million was online banking fraud. FFA UK also provided estimates on other categories of non-online fraud, discussed how fraud is generally committed, and provided safety tips for consumers. It did not provide any details, however, on how the estimates or costs were collected and tabulated.

In addition, the report provided a summary of all the measures that the card industry has taken over the last decade that have reportedly reduced the losses associated with fraud. No estimates were provided on how much has been spent on these actions. Some of the measures discussed in the report were:

- the Dedicated Card and Payment Crime Unit (DCPCU), stated to have saved £470 million since its inception;
- the Financial Fraud Bureau (FFB);
- the Fraud Intelligence Sharing System (FISS);
- American Express Safekey,
- MasterCard SecureCard;
- Verified by Visa;
- Address Verification Services (AVS) and Card Security Code (CSC);
- Cyber Streetwise;
- Chip and Pin, banks' use of intelligent fraud detection systems;
- industry measures to prevent cash machine crime;
- industry measures to protect customers from cheque fraud; and
- industry measures to prevent online and telephone banking fraud.

Estimates on the costs of these measures would provide further knowledge on the anticipation/prevention costs of various forms of fraud.

The data reported by FFA UK likely represent some of the most reliable data currently available with which to begin to consider the overall cost of cyber crime to the UK. This is due to FFA UK data being collated from information provided directly to them by banks, credit, debit and charge card issuers, and card payment acquirers in the UK, regarding all their actual fraud cases and associated losses. These data are collected in line with industry agreed definitions and categories, and in addition to allowing the FFA UK to generate estimates, contribute to the discussion around how fraud is generally committed, and provide safety tips for consumers.

The FFA UK report lacks detail however on how the reported figures and costs are collected and tabulated. In addition, the report provided a summary of a number of measures that the card industry has taken over the last decade that have reportedly reduced the losses associated with fraud. For example, the Dedicated Card and Payment Crime Unit (DCPCU) is stated to have saved £470 million since its inception. No estimates were provided on how much has been spent on these actions. Estimates on the costs of these measures would provide further knowledge on the anticipation/prevention costs of various forms of fraud.

British Retail Consortium, 2015

The British Retail Consortium (BRC) reports that the total cost of crime to the UK retail sector was £603 million in 2013–2014, an increase of 18 per cent; £223 million of this were losses as a result of fraud. It estimated that 69 per cent of credit/debit card fraud, 33 per cent of account credit fraud, 10 per cent of refund fraud, and 10 per cent of voucher/gift card fraud was committed online. The report also found that the majority of respondents indicated that the level of cyberattacks remained either the same or had increased. Additionally, a majority of respondents found the following threats to be critical:

- theft of data (77%);
- hacking (68%);
- denial of service attack (64%);
- site scraping (64%);and
- malicious software (55%).

The BRC's report does not provide detailed specifics on how its sample was created, but states that its *"sample covered 50 per cent of the retail sector by turnover and employed 1.6 million employees"* (p 10). Given the lack of detail available describing the research methods used, it is unclear how reliable the results generated by this survey are and how representative they are of retail population as a whole, and, as such, whether the extrapolations made are valid.

The National Fraud Authority, 2013

The National Fraud Authority (2013) was also interested in providing estimates for fraud losses across many sectors. It worked with stakeholders in various sectors and created overall estimates by collecting primary data from surveys and secondary data from its partners. NFA estimates were not necessarily comparable from year to year because of improvements with methodology; its estimates should therefore be viewed more as a *"best estimate of the possible size of the problem"* (p 4). It should also be noted that the estimates presented in the NFA report make use of:

- secondary data, not all of which are robust;
- data from non-random probability sample surveys, which are therefore unlikely to be representative of the population being researched; and
- mean average loss data, which are likely to be skewed by anomalies.

The 2013 report estimated the cost of fraud to the UK economy at £52 billion. This figure, among many others in the report, is generally not broken down between online and offline fraud. For example, the National Fraud Authority estimated that the direct and hidden costs to large and small/medium corporations in the private sector because of fraud per annum were £6.7 billion and £9.2 billion respectively. In addition, it estimated that the direct and hidden costs to the public sector as a result of fraud was £20.6 billion. This figure focused mostly on tax revenue, benefits, and grants and did not include costs of law enforcement initiatives. Charities were defrauded £147.3 million in both online and offline fraud, including payment fraud, fraud by employees or volunteers, and cyberfraud.

Other estimates provided a little more insight into the proportion of the fraud type that was cyber-enabled. For example, it estimated that the loss to financial sector for fraud per annum was £5.4 billion; £40 million of this was considered to be online banking fraud and £388 million was plastic card fraud. Individuals were estimated to have lost £9.1 billion as a result of fraud per year. The National Fraud Authority divided this estimate into:

- mass marketing fraud at £3.5 billion (with much of it possibly being cyber);
- identity fraud at £3.3 billion (much of which could also be cyber);
- online ticket fraud at £1.5 billion (all cyber);
- private rental property fraud at £755 million; and
- pre-payment meter scams at £2.7 million.

Security providers

Over recent years, it has become common for security providers to create estimates on the costs of cyber crime that support the need for their products. As with all reports published by software producers/suppliers, readers need to be aware that such reports are produced that typically reinforce the need for/value of the products they offer. A wider range of limitations with security reports measures are also noted in Home Office (2013c).

The McAfee/Intel report (2014) attempted to create estimates on the global cost of cyber crime. They write that their estimate: *"looks at both direct and indirect costs, and data used that takes into account the loss of intellectual property, the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including the reputations damage to the hacked company"* (p 4).

McAfee/Intel also consider estimates surrounding stolen intellectual property to be challenging. They write: *"the cost of stolen Intellectual Property (IP) is the most difficult to estimate for the cost of cyber crime, but it is also the most important variable for determining loss"* (p 6).

Based on this framework, they report that the global cost of cyber crime is either:

- $375 billion (considered conservative and estimated by extrapolating open source data);
- $445 billion (estimated by aggregating costs as a share of regional incomes); or
- a top estimate of $575 billion (extrapolating data from loss by high-income countries).

In addition, they estimate that the proportion of UK GDP that is lost due to cyber crime is 0.16 per cent, which they provide a low ranking of confidence. They do not, however, provide their evidence for this estimate. The report also draws on previous research, e.g.

Anderson *et al* 2012 rather than new primary research.
In contrast, Symantec (2013) reported much lower estimates. Symantec conducted an online survey with over 13,000 adults aged 18-64 in 24 countries. It should be noted that the usual limitations regarding online survey samples apply to this research. We cannot be confident that the survey is representative of the wider population when conducted in this fashion. The UK sample was weighted to represent 500 adults. Symantec reported that the global (based on 24 countries) total cost of cyber crime in the past 12 months was US$113 billion for an average direct cost per cyber crime victim of US$298. For the UK, it estimated that the total cost of cyber crime over the past 12 months was US$1 billion, with an average direct cost per cyber crime victim of US$101. The report estimated there were 12 million victims in the 12 months prior to the survey. McAfee/Intel, report that they believe they may have underestimated the cost of cyber crime because of intangibles and the 'true' cost to both the global economy and national security.

Verizon (2015) reported financial cost predictions for companies that had data breaches based on the number of records stolen. In its report covering information on 70 contributing organisations in 61 countries during 2014 there were:

- 79,790 security incidents (defined as any event that compromises the confidentiality, integrity, or availability of an information asset); and
- 2,122 confirmed data breaches (defined as an incident that resulted in confirmed disclosure, not just exposure, to an unauthorised party).

Although Verizon found that no industry was immune to data breaches, public, information, and financial services industries experienced the most confirmed data loss security breaches. In addition, it provided predicted estimates of data breaches based on the size of the breach as measured by number of records stolen (100; 1,000; 10,000; 100,000; 1,000,000; 10,000,000; 100,000,000). For example, $1,258,670 is the expected financial cost to companies for a data breach with 1 million records stolen (average between $892,400 and $1,775,350 and prediction between $57,600 to $27,500,090).

Neustar (2015) found that half of businesses reported that denial of service or distributed denial of service (DDoS) attacks were a bigger threat than a year ago. Interestingly, a majority of companies that reported that DDoS attacks were a smaller threat now had still invested more in protecting their companies against these attacks. Over a quarter of the companies reported that brand/customer trust was the issue that was most affected by DDoS attacks. When hit, one in three companies reported that the attack lasted for one to two days. Half of the companies that were attacked were also victims of theft of either customer data, intellectual property, or funds. In Neustar's sample of 250 professionals, it found that 22 per cent of the companies reported revenue losses between £50,000 and £99,999 per hour due to outages at peak times, making it the most common response option. In addition:

- 16 per cent reported that their losses per hour were less than £30,000;
- 12 per cent reported losses between £30,000 and £49,999;
- 16 per cent between £100,000 and £299,999;
- 11 per cent between £300,000 and £600,000;
- 12 per cent greater than £600,000; and
- 11 per cent did not know what their outages cost them.

City of London Police (2015)

In the City of London Police (2015) report on the implications of economic cyber crime for policing, the authors focused on three main forms of economic cyber crime:

- cyber-dependent crimes;
- cyber-enabled crimes; and
- cyber-assisted crimes.

In investigating these forms of cyber crimes the authors conducted original research on an extract of Action Fraud data, from which they reported a number of findings. These include estimates of the median amounts given to fraudsters by victims in the fourth quarter of 2014 – for example:

- £38,974 for pension fraud;
- £28,609 for business trading fraud;
- £21,534 for financial investment fraud; and
- £20,000 for bankruptcy and insolvency fraud.

The report also provides estimates for the (mean) average amounts recovered from fraudsters during the fourth quarter, for example:

- £39,958 for financial investment fraud;
- £47,542 for banking and credit industry fraud;
- £35,863 for corporate fraud; and
- £30,904 for pension fraud.

A number of other estimates are provided based on the primary analysis of the data extract, which can help researchers to understand the nature of frauds reported within the sample.

While the research presented in this report provides a useful context when considering the types and magnitude of frauds reported, there are a number of technical and methodological considerations that affect the level of confidence that can be attributed to the reported estimates.

For example, it was not always clear whether the analysis was based on crimes or incidents (inclusion of incidents could adversely affect the reliability of any subsequent results). The analysis also defined ‘cyber-involvement’ as based on the method of first contact, which may not be the most robust proxy. To provide an example of how this might not be the most robust proxy: using this definition ‘hacking server’ only has 31 per cent for the ‘proportion of cyber-involvement’, whereas given the nature of this offence it would be reasonable to expect 100 per cent cyber-involvement. Additionally, the use of ‘cyber-assisted’ as a subset of cyber crimes means that the results of this study are not easily comparable with other studies, which have tended to use definitions that are more consistent across the extant literature (for example, cyber-enabled and cyber-dependent crimes).

The self-reported victim cost data also need to be treated with caution as they are susceptible to misreporting, and reflect losses only at the time of initial reporting; they do not take into consideration subsequent compensation payments. The volume of missing data more broadly in the Action Fraud dataset is also a limitation.

Overall, this impacts on the level of confidence that can be attributed to the reported estimates, but represents a useful avenue for further exploration.

Offender revenues

Though the Costs of Cyber Crime Working Group felt that it was important to look at costs from various different perspectives, to date, there has not been a heavy focus on examining the revenues associated with cyber crime. During this work programme the Working Group considered incorporating offender costs/revenues into the costs of cyber crime framework. However, it was not considered to be a suitable fit. In light of these challenges, as this report indicates, the primary focus of cyber crime cost reports is examining the costs accrued by both corporations and individuals.

In this chapter an exhaustive review of reports examining offender revenues is not provided as it is not directly tied to cyber crime costs. In other words, the costs associated with a crime are not the same as the profits gained by an offender. In most cases, the direct consequential costs of the cyber crime will be much higher than the offender revenues, even without considering anticipation and response costs. In this section, the findings from Anderson *et al*. (2012), Symantec (2015), and the Ponemon Institute (2016) are considered*.* Most of these estimates should be taken with extreme caution as the estimates were:

- based on expert perceptions of profits rather than cybercriminal surveys;
- extrapolated from small sample sizes, or
- extrapolated from global figures.

The Anderson *et al*. (2012) report provided revenue amounts for a wide variety of cyber-enabled and cyber-dependent crimes. They estimated that the monthly revenue of counterfeit pharmaceuticals sales in 2010 was $8 million per month or $288 million for the year globally. Using the *“UK 5% estimate of the world GDP rule,”* they estimated that UK consumers *“provided roughly $400,000 to the top counterfeit pharmaceutical programs in 2010 and perhaps as much as $1.2M per month overall”* (p 13) or $14 million over the year. Regarding counterfeit software, they estimated that the top five learning counterfeit software organisations made $22 million worldwide in 2011 with an estimate of $1 million from the UK. The global figure for proceeds of copyright-infringing music and video was estimated at $150 million ($7 million from the UK) by examining the asset seizures of the Megaupload gang in Auckland and multiplying it by its share of the market. Global revenue from fake antivirus software was estimated to be at $97 million with the UK share of that being 5 per cent.

Anderson *et al*. also examined revenue from different types of scams, including stranded traveller, fake escrow, and advanced fee fraud scams. They estimated that the revenue for stranded traveller scams is *"most unlikely to exceed $1 million per annum"* (p 15) in the UK, based on unpublished data primarily involving US victims. With roughly 100 active fake escrow websites at any one time, they estimated UK losses as a result of fake escrow scams to be in the order of $10 million per year. Finally, they reported that advanced fee fraud scam *“seem*[s] *likely that it is more lucrative than the stranded traveller and fake escrow scams"* (p 16). They estimated these losses to be $50 million, but they write, *“we would be the first to admit that this figure is merely indicative and we have no real evidence to support it”* (p 16).

Symantec (2015) reported on the value of certain products in the underground economy. It stated that, *"overall, email prices have dropped considerably, credit card information has declined a little, and online bank account details have remained stable"* (p 88). It also concluded that *"prices are holding steady in the underground economy, suggesting continuing high levels of demand for stolen identities, malware, and e-crime services"* (p 88). Symantec provided the following values of different types of information sold on the black market in 2014:

- 1,000 stolen email addresses were $0.50 to $10;
- credit card details ranged from $0.50 to $20;
- scans or real passports had values of $1 to $2;
- stolen gaming accounts could fetch $10 to $15;
- custom malware ranged anywhere from $12 to $3,500;
- 1,000 social network followers would cost $2 to $12;
- stolen cloud accounts were valued at $7 to $8;
- 1 million verified email spam mail-outs had only cost $70 to $150; and
- registered and activated Russian mobile phone SIM cards were valued at $100 (p 89).

The Ponemon Institute (2016) surveyed 304 threat experts who resided in the US, UK, and Germany who considered themselves:

- familiar with present-day hacking methods;
- experienced in successfully penetrating computer systems; and
- involved in the hacker community.

A majority of these experts – 69 per cent – stated that financial reasons were the primary motivation for computer attacks. They estimated that attackers earned $28,744 annually – only one-quarter of a cybersecurity professional's annual yearly wage. They viewed attackers as opportunists who chose the easiest targets first; 72 per cent believed that attackers will not spend their time on attacks that will not quickly result in high-value information. A similar proportion of the experts (69%) suggested that hackers quit the attack when the organisation presents a strong defence. A typical attacker may spend 70 hours to plan and execute an attack against an organisation with a normal security infrastructure but may spend more than 6 days (147 hours) to plan and execute the same attack against an organisation with an excellent IT infrastructure.

A concerning finding was that half of the experts believed that the attacker's total cost of successful attacks, as well as the time to plan and execute an attack, had decreased, which would only increase the amount of attacks against various industries. A majority of the experts who viewed successful attacks as becoming easier saw the number of vulnerabilities and exploits as well as the hacker skill levels increasing. The Ponemon Institute suggested that investments in security effectiveness would significantly reduce successful attacks because this would increase the effort required by attackers. As with other Ponemon studies, it discussed the limitations of its web-based surveys, which include non-response bias, sampling-frame-bias, and issues surrounding self-reported results (p 16).

Appendix 2: Glossary of the terms used in the costs of cyber crime framework

Terms	Definitions
Additional costs to the probation system	Direct costs of supervising cyber criminals on probation. There are opportunity costs as well since the funds and time could have been spent monitoring other types of criminals or have been used for other governmental priorities.
Avoidance of the internet and/ or other technologies (amongst non-users)	Fear of cyber crime e.g. from publicised media incidents, may cause concern about victimisation amongst those who don't already use the internet or other technologies. This may then cause them to avoid these technologies all together and resort to use of traditional, offline technologies.
Business disruption (including lost output)	Loss of business revenue during and in the immediate aftermath of a cyberattack caused by inability of a business to function as normal (e.g., websites down or running slowly as a result of DDoS attack, online businesses being unable to make sales). This includes costs of lost productivity of employees not being able to work as productively because of the attack.
Checking credit histories/scores	Additional direct monetary costs incurred by individuals, companies, and government entities in checking credit histories/scores to enable early identification of any fraudulent use of personal information. This also includes the opportunity cost of time spent by individuals, companies such as lenders, and government entities that could have been used more productively.
Clean-up expenditures	Direct and opportunity costs of time and money spent fixing the security problems or the damage and / or addressing causes of the attack. Clean-up costs may be incurred by a variety of parties, from individuals through to businesses, internet service providers and security companies.
Collection and compilation of cyber crime statistics	Direct costs of law enforcement agencies at all levels (local, national) to collect, compile, and report statistics on different forms of cyber crime. This includes costs relating to Action Fraud as the national reporting centre for cyber crime and fraud. There are opportunity costs as well since law enforcement could utilise the funds and time to collect and analyse statistics on different crimes or simply use the funds and time for other priorities. Also includes direct costs of non-law enforcement agencies (e.g., national non-law enforcement governmental agencies, e.g. the Office for National Statistics) in collecting, compiling, and reporting statistics on different forms of cyber crime. There are opportunity costs as well since these non-law enforcement entities could have used the funds and time for other priorities
Computer security protection software/products	Direct costs of expenditures on anti-virus and other computer security protection software/products as well as opportunity cost of the expenditure as the individual, company, or government entity could have spent the funds on other products that may have been more

	productive or needed. Direct cost of patching software to address vulnerabilities is also included. Opportunity costs exists as well as the expenditure of funds and time/productivity could have been spent on other issues.
Consumer credit/identity protection services (e.g. CIFAS)	Direct monetary and opportunity costs associated with the amount that individuals spend on protection services with companies to secure/protect their credit or identity.
Costs as a consequence of cyber crime	Costs that occur as a result of the crime (e.g. costs arising from money lost or IT systems damaged). These are costs for which you have little / no control over.
Costs as a response to cyber crime	Costs occurring as a result of your decision regarding what to do in response to a specific crime (e.g. bringing in law enforcement). These are costs where you have more control over as there are more decisions to be made about what to do. This does not include general responses to cyber crime e.g. an awareness campaign introduced by government as a generalised response to cyber crimes.
Costs in anticipation or prevention of cyber crime	Measures taken to reduce the risk or likelihood of victimisation, involving defensive and precautionary behaviours (e.g. spend on anti-virus, cyber security training courses).
Cyber-dependent crimes	Offences that can only be committed using a computer, computer networks or other forms of information communications technology, considered 'pure' cyber crimes (Home Office, 2013c).
Cyber-enabled crimes	Traditional crimes which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike cyber-dependent crimes, they can be committed without the use of ICT (Home Office, 2013c).
Cyber insurance administration	Cyber insurance protection plans generally cover liability issues related to network security breaches. Costs here only relate to administration costs of the insurance and not the cost of insurance itself because. (This is because the only resources involved in insurance that represent a cost of crime to society rather than a transfer are the resources used in insurance administration. Insurance companies require staff, premises and equipment in order to provide, check and pay out on policies. The resources used in insurance administration represent an opportunity cost to society, because in the absence of crime these resources could be employed in a productive way elsewhere in the economy.)
Cyber-security training/education	The monetary costs of providing and undertaking cyber-security training/education for both employees and consumers / members of the general public. This may include costs in time spent developing knowledge / understanding what the threats are and developing appropriate skills to tackle them. Opportunity costs include the funds and time that could have been spent on other issues or different types of training.
Damage to reputation or brand value	Losses associated with decreased business reputation or brand value because of cyberattack. This includes, but is not limited to, loss of company value (e.g., stock value), future lost revenues, loss of trust and confidence in brands / companies. This also include damage to

	reputation, loss of trust / confidence in government and law enforcement.
Disputed transactions	Monetary and opportunity costs of time and legal fees by individuals and companies to investigate and settle disputed claims from consumers.
Drafting and creating new legislation	The costs, primarily opportunity costs, of creating new legislation to address cyber crime. This is mostly an opportunity cost as their time and other resources could have been used to address other societal issues.
Efforts to educate public on new legislation	Direct costs of advertising the new legislation (e.g., websites, media, etc.), but also the opportunity costs associated with the resources and time that was used to educate the public on new legislation that could be allocated elsewhere.
Emotional/physical harms	The direct and opportunity costs associated with treatment of emotional and physical health issues as a result of cyber victimisation.
Equipment/infrastructure damage	Direct cost of the equipment/IT/infrastructure damage.
Fear / worry about cyber crime	Fear / worry about cyber crime that causes emotional or physical impacts on quality of life.
Implementation of national awareness raising / protection campaigns	Direct costs of national awareness raising / protection campaigns instigated by government and/ or other bodies and designed primarily to decrease victimisation amongst the general public, consumers but also amongst businesses (e.g., Cyber Streetwise, GetSafeOnline). This is regarded as a response cost because they are typically undertaken as a response to cyber victimisation in order to protect from further incidents in future. This also involves opportunity costs as these funds and the time spent developing these campaigns could have been used to address other issues.
Implementing cyber security practices	Opportunity costs of the time spent implementing cyber security practices, such as updating software and checking authenticity of emails / websites. This item is not looking at the time associated with training and/or educating individuals on proper cyber security protection.
Incarceration of cyber criminals	Direct costs of incarcerating individuals convicted of a cyber crime as well as opportunity costs that the resources could have been allocated differently to incarcerate a different type of offender or use for a different governmental priority.
Increased / improved IT spending as a direct response to victimisation	Monetary and opportunity costs of increased IT spending that is above normal operating procedures as a result of cyber crime, this also includes improved expenditure e.g. on better equipment / technology / protection software. This are things introduced as a direct response to cyber crime victimisation (rather than in anticipation).
Introduction of new / additional technologies	Expenditures on newer technologies to reduce cyber crime, such as fraud (e.g., EMV credit cards, secure email). Opportunity costs exist as well since the funds could have been spent differently on other priorities.

Law enforcement and disruption activities	Expenditures on law enforcement preventing, disrupting, and investigating cyber crimes. This includes the NCA, Regional Organised Crime Units, and Local Police activity. Examples include, but are not limited to spend related to: website takedowns, labs, digital forensics software, and day-to-day- investigators / investigation costs. There are also opportunity costs because: (1) the law enforcement personnel could be using their time and resources to address other forms of crime; and (2) the government providing the funds to law enforcement to address cyber crime could have spent the funds on different priorities.
LBEs	Large Business Entities: business entities that are larger than the criteria set forth for small and medium business entities. See definition of SME.
Legal, PR advice and similar expenses	Monetary and opportunity costs of legal advice, PR advice and similar expenses (e.g., travel) that consumers, companies, government agencies, and other entities accrue as a result of responding to cyber crime (e.g., hiring a lawyer or PR team to resolve disputes or negative publicity caused by cyber crime).
Lost value of IP/commercially sensitive information	Value of the intellectual property or commercially sensitive information stolen during a cyberattack. Although this may be estimated as the value of the intellectual property or commercially sensitive information if sold on the open market, it may also be estimated as the damage to the company's competitiveness because of the loss.
Monetisable costs	Impacts that can be readily expressed in cash terms, i.e. where market value / price can be used to establish cost (e.g. cost of stolen property or damage to equipment which has an identifiable price).
Monitoring of third parties' security	Monetary costs of monitoring the security precautions/procedures of third parties as well as the opportunity costs involving the funds and time that could have been spent on other priorities.
Non-monetisable costs	Where impacts cannot be readily expressed in cash terms, i.e. there is no market value /price available and we therefore need to estimate costs using other data (e.g. business reputation, emotional or physical harms).
Online theft/fraud of funds	Amount of funds stolen via theft or fraud online. There are opportunity costs as well as these funds could have been invested into the company to develop growth.
Opportunity cost	All choices have an opportunity cost; it is assumed there is always another use for the resource. If resources are put towards use A rather than use B, the value of B is known as the opportunity cost. For example, if a business has £100 to invest, and wants to invest in software costing £100, or marketing costing £100, a choice must be made. If software is chosen, the value of the marketing is the opportunity cost. The opportunity cost of things such as purchasing anti-virus software, or employing someone new to recover damaged files will be captured in the market price. This is because these are new financial transactions.
Prosecuting cyber cases	Direct costs of the process, proceedings, and trial (judge, prosecutor, public defender), including investigations completed by the prosecutor,

	and the opportunity costs that the resources and time could have been used to address other crimes.
Rectifying credit histories / scores	Direct monetary costs and time incurred by individuals, companies, and government entities in rectifying credit histories/scores caused by any fraudulent use of personal information.
Reduction in R&D spending	Cost arising as response from cyber crime, driven by a firms' lack of future ambition to innovate or invest in Research and Development if they cannot ensure that their IT systems are secure enough to prevent future attacks.
Reporting/documenting incidents	Direct and opportunity costs of consumers, companies, and non-government agencies collecting and documenting cyber incidents to report to various entities, this also includes trying to establish cause, time taken following internal company procedures / requirements and those required from the entities being reported to etc.
SMEs	Small and medium-sized enterprises: For a company to be defined as an SME in the UK, it needs to meet two of three criteria: (1) turnover of less than £25m, (2) has less than 250 employees; and (3) has gross assets of less than £12.5m. Definitions of what constitutes an SME vary among government agencies.
Switching ISPs, security providers or products to increase security	Direct costs arising from switching ISPs, security providers or other security related products (e.g., administrative fees, increased product prices) as well as the opportunity costs involving the time switching.
Switching ISPs, security providers or products as a direct response to victimisation	Direct costs arising from switching ISPs, security providers or other security related products (e.g., administrative fees, increased product prices) as well as the opportunity costs involving the time switching. Occurring as a direct result of cyber crime victimisation rather than in anticipation.
Training / education put in place as a direct response to victimisation	Training and education that has been provided / undertaken by businesses and individuals as a response to cyber crime victimisation (rather than in anticipation).
Training for law enforcement investigators and officers	Expenditures on the training of investigators and constables to respond to and investigate various forms of cyber crime. This item includes opportunity costs as well since the funds and time could have been used differently by law enforcement, including training on other issues.
Training of court and legal personnel	Expenditures on cyber crime training (e.g., what it is, prevalence, statutes, etc.) for court personnel (e.g., judges, prosecutors, public defenders, etc.). There is opportunity costs as the funds and time could have been used for different forms of training or other governmental priorities.
Usability/user impact as a result of increased security procedures	Lost productivity time for user (e.g., employee, individual) due to increased security precautions.
Vetting of staff or contractors for security purposes	Direct costs incurred by companies, organisations, or entities to vet individuals and contractors for security purposes. This would include either the entity conducting the extra vetting procedures themselves or

	paying a vetting company. There are opportunity costs as well since the funds and time could have been spent differently by the entity. In addition, there are opportunity costs for the person or entity being vetted regarding loss productivity time or possibly delayed profits.
Victim support services	The direct and opportunity costs of the funds that are spent by both the government and businesses on cyber victim support services. This may also include wider support, e.g. from health services in tackling emotional / physical impacts.

Appendix 3: Draft measures to estimate the value of business reputation

The following draft quantitative measures were designed in order to be added to business questionnaires, to help quantify the value of business reputation. This will help researchers to assess the impact of cyberattacks on business reputation. These questions would require further cognitive testing and development before being used to collect data in support of future robust studies measuring the costs of cyber crime.

Questions for businesses with experience of cyber crime

1) **Number of times experienced each type of cyber crime –** this is important because it feeds into the level of public/customer tolerance for cyber crime.

Q1. [ASK ALL]

In the last 12 months how many times, if any, has your business experienced each of the following types of cyber crime?

A. Infection by viruses or malicious software (Malicious software)
B. Unauthorised access to company data or information held by the business (Hacking/computer intrusions)
C. Disruption to your corporate website (DDOS attacks)
D. Defacement of your corporate website (Website defacement)
E. Use of the business' information or account details to obtain money or buy goods or services without the authorisation of your business (Fraud/theft)
F. Tricked or deceived out of money or goods (Fraud/theft)
G. Theft of intellectual property (Intellectual property theft)
H. Something else (please specify)
I. None of these
J. Don't know (SPONTANEOUS ONLY)

2) **Nature of cyber crime experienced –** this is a summary question that maps the answer categories to the costs of cyber crime framework.

The nature of the cyber crime is important in determining the impact of the crime on a business and will provide a way to break down the potential impact by type of cyber crime.

Q2. [ASK IF EXPERIENCED MORE THAN ONE TYPE OF CYBER CRIME]

Which of the following best describes the **most recent** incident of cyber crime experienced by your business?

A. Infection by viruses or malicious software (Malicious software)
B. Unauthorised access to company data or information held by the business (Hacking/computer intrusions)
C. Disruption to your corporate website (DDOS attacks)
D. Defacement of your corporate website (Website defacement)

E. Use of the business' information or account details to obtain money, or buy goods or services without the authorisation of your business (Fraud/theft)
F. Tricked or deceived out of money or goods (Fraud/theft)
G. Theft of intellectual property (Intellectual property theft)
H. Something else (please specify)
I. None of these
J. Don't know (SPONTANEOUS ONLY)

Q2b. [ASK IF EXPERIENCED MORE THAN ONE TYPE OF CYBER CRIME]

And which of the following best describes the **most serious** incident of cyber crime experienced by your business?

A. Infection by viruses or malicious software (Malicious software)
B. Unauthorised access to company data or information held by the business (Hacking/computer intrusions)
C. Disruption to your corporate website (DDOS attacks)
D. Defacement of your corporate website (Website defacement)
E. Use of the business' information or account details to obtain money, or buy goods or services without the authorisation of your business (Fraud/theft)
F. Tricked or deceived out of money or goods (Fraud/theft)
G. Theft of intellectual property (Intellectual property theft)
H. Something else (please specify)
I. None of these
J. Don't know (SPONTANEOUS ONLY)

[IF MOST RECENT AND MOST SERIOUS INCIDENT ARE DIFFERENT ALL OF THE FOLLOWING QUESTIONS SHOULD BE ASKED ABOUT THE MOST RECENT INCIDENT FOLLOWED BY THE MOST SERIOUS INCIDENT]

3) Extent of publicity surrounding the cyberattack

Q3. [ASK ALL]

How would you best describe the extent of publicity surrounding the **most recent** incident of cyber crime experienced by your business?

- In depth media coverage
- Limited media coverage
- No media coverage
- Don't know (SPONTANEOUS ONLY)

And how would you best describe the extent of publicity surrounding the **most serious** incident of cyber crime experienced by your business?

Q4. [ASK ALL]

To the best of your knowledge which of the following people were aware of the **most recent** incident?

A. No one aware outside of a few senior people within the business
B. A small number of employees
C. A wide range of employees in the business
D. Business partners and potential partners
E. Investors, funders or shareholders
F. Competitors
G. A small number of existing or potential customers
H. A wide range of existing or potential customers
I. General public
J. Someone else (please specify)
K. Don't know (SPONTANEOUS ONLY)

And to the best of your knowledge which of these people were aware of the **most serious** incident?

4) Level of impact of cyber crime

Q5. [ASK ALL]

Was any confidential data accessed as a result of the **most recent** cyber crime experienced?

1. Yes
2. No
3. Don't know

And was any confidential data accessed as a result of the **most serious** cyber crime experienced?

Q6. [ASK IF Q4=G OR Q4=H]

To the best of your knowledge did any of your customers experience any financial loss as a result of the **most recent** cyber crime experienced?

1. Yes
2. No
3. Don't know

And to the best of your knowledge did any of your customers experience any financial loss as a result of the **most serious** cyber crime experienced?

5) Impact on reputation

Q7. [ASK ALL]

What, if any, impact do you think the **most recent** incident had on the level of trust[22] in your business among your existing customers?

1. Increased a lot
2. Increased a little
3. No change
4. Decreased a little
5. Decreased a lot
6. Don't know (SPONTANEOUS ONLY)

And what, if any, impact do you think the **most serious** incident had on the level of trust in your business among your existing customers?

Q8. How important do you feel that the cybersecurity of your business is to your customers?

1. Very important
2. Fairly important
3. Not very important
4. Not at all important
5. Don't know (SPONTANEOUS ONLY)

Q9. To what extent do you believe that your business reputation was damaged by the **most recent** incident of cyber crime?

1. To a great extent
2. To some extent
3. No extent
4. Don't Know (SPONTANEOUS ONLY)

And to what extent do you believe that your business reputation was damaged by the **most serious** incident of cyber crime?

Cost estimates

Q9. [ASK ALL]

I would like to ask you about the costs associated with any damage to your business reputation following the **most recent** incident. What would you estimate was the cost of damage to your business reputation in terms of any loss of revenue, direct costs related to handling the incident and any professional time costs associated with dealing with the incident?

So firstly, what would you estimate was the cost of damage to your business reputation in terms of any loss of revenue?

[22] Trust used here as a proxy for reputation.

Loss of revenue might include any loss of existing business or loss of potential business.

Please give your best estimate.

[ENTER ESTIMATE]

Don’t know

And what about any loss of revenue costs associated with any damage to your business reputation following the **most serious** incident?

[ENTER ESTIMATE]

Q10. [ASK ALL]

And what would you estimate was the cost of damage to your business reputation in terms of any direct costs related to handling the **most recent** incident?

Direct costs might include:

- any IT costs associated with dealing with the incident
- any other Incident management costs
- legal fees
- discounts or reimbursements provided to consumers as compensation for the incident

Please give your best estimate.

[ENTER ESTIMATE]

Don’t know

And what would you estimate was the cost of damage to your business reputation in terms of any direct costs related to handling the **most serious** incident?

[ENTER ESTIMATE]

Q11 [ASK ALL]

What would you estimate was the cost of damage to your business reputation in terms of any professional time costs related to handling the **most recent** incident?

Professional time costs would include time taken by staff within the business to deal with the incident.

Please give your best estimate.

[ENTER ESTIMATE]

Don’t know

And what would you estimate was the cost of damage to your business reputation in terms of any professional time costs related to handling the **most serious** incident?

[ENTER ESTIMATE]

Q12 [ASK IF PUBLIC LIMITED COMPANY]

What would you estimate was the cost of damage to your business reputation in terms of any reduction in share price related to the **most recent** incident?

Please give your best estimate.

[ENTER ESTIMATE]

Don’t know

And what would you estimate was the cost of damage to your business reputation in terms of any reduction in share price related to the **most serious** incident?

[ENTER ESTIMATE]

Q13 [ASK ALL]

What would you estimate was the cost of damage to your business reputation in terms of any other costs related to handling the **most recent** incident?

Please give your best estimate.

[ENTER ESTIMATE]

Don’t know

And what would you estimate was the cost of damage to your business reputation in terms of any other costs related to handling the **most serious** incident?

[ENTER ESTIMATE]

Alternative proposal v1

Two proposals were considered during the project. This second proposal could be used instead of the initial proposal. Further testing and development is required in order to identify which proposal would be best suited to future research work investigating the costs of cyber crime.

I would like to ask you about the costs associated with any damage to your business reputation following the incident. What would you estimate was the cost of damage to your business reputation in terms of the following costs?

- Loss of revenue (for example, loss of existing business, or potential new business, caused by publicity/awareness surrounding the breach)?
-
  - ○ [ENTER ESTIMATE]
  - ○ Don’t know

- Costs from lost investor or funder support due to publicity/awareness of the breach?
  - [ENTER ESTIMATE]
  - Don't know

- Costs related to handling the incident (for example, PR fees; staff time dedicated to customer services, providing information about the incident or handling complaints and queries)?
-
  - [ENTER ESTIMATE]
  - Don't know

- Costs from 'goodwill' compensation payments or discounts provided to customers?
  - [ENTER ESTIMATE]
  - Don't know

- [IF PUBLIC LIMITED COMPANY] Reduction in share price?
  - [ENTER ESTIMATE]
  - Don't know

- Any other costs relating to business reputation?
  - [ENTER ESTIMATE]
  - Don't know

ALTERNATIVE PROPOSAL v2

Two proposals were considered during the project. This second proposal could be used instead of the initial proposal. Further testing and development is required in order to identify which proposal would be best suited to future research work investigating the costs of cyber crime.

I would like to ask you about the costs associated with any damage to your **business reputation** following the incident. What would you estimate was the cost of damage to your business reputation in terms of the following costs?

- Loss of revenue (for example, loss of existing business, or potential new business, caused by publicity/awareness surrounding the breach) or loss of investment due to awareness of the breach?
-
  - [ENTER ESTIMATE]
  - Don't know

- Costs related to handling the incident (for example, PR fees; staff time dedicated to customer services, providing information about the incident or handling complaints and queries including any compensation payments made)?
-
  - [ENTER ESTIMATE]
  - Don't know

- Any other costs relating to business reputation?
  - [ENTER ESTIMATE]
  - Don't know

Appendix 4: Signposting to more detailed report summaries of research commissioned by the Working Group

Furnell, S. (2016). "*The Evolving Landscape of Technology-Dependent Crime*", in The Routledge Handbook of Technology, Crime and Justice. M.R.McGuire and T.J.Holt (Eds), Routledge International Handbooks. See https://www.routledge.com/The-Routledge-Handbook-of-Technology-Crime-and-Justice/McGuire-Holt/p/book/9781138820135

Furnell, S; Emm, D and Papadaki, M. (2015). *"The challenge of measuring cyber-dependent crimes"*, Computer Fraud and Security, October 2015, pp5-12. See http://www.sciencedirect.com/science/article/pii/S1361372315300932

Furnell, S. (2015). *"Getting the measure of cyber crime?"* University of Oxford, 5th June 2015 https://itunes.apple.com/us/podcast/getting-measure-cybercrime/id402420124?i=1000355139549&mt=2

Holt, T. J., Smirnova, O. and Chua, Y. T. (2016) "Exploring and estimating the revenues and profits of participants in stolen data markets", *Deviant Behavior,* 37 (4) pp 353–367.

Smirnova, O. and Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist* 61(11): 1403-1426.

Appendix 5: Costs of Cyber Crime Working Group Terms of Reference

TERMS OF REFERENCE

1.0 Context

1.1 The Costs of Cyber Crime Working Group ('the Working Group') was established to meet requirements outlined in the Home Office Serious and Organised Crime Strategy to obtain a better understanding of the scale and costs of cyber crime. Whilst acknowledging the challenges of providing accurate estimates, the Strategy stated:

> *"Based on the limited evidence available, the costs of cyber crime in the UK are likely to be at least several billions of pounds each year. A new external Working Group is being set up by the Home Office to improve data quality in this area."* (Home Office, 2013a)

1.2 Prior to the Strategy, the Home Affairs Select Committee (HASC) also expressed concern over the lack of accurate and up-to-date figures measuring the scale and cost of cyber crime and recommended the set-up of an external group of industry and academics to improve such estimates.

1.3 Gaining a better understanding of both prevalence and costs of cyber crime would help to:

- understand the nature of the cyber crime threat and how it is changing over time;
- raise awareness of cyber crime amongst law enforcement and ensure resources are directed at priority crime types; and
- ensure that awareness and prevention activities are directed towards those individuals and businesses that are more vulnerable.

1.4 Broadly, the Working Group is interested in:

- where different costs fall (for example, in terms of anticipation, direct costs or in response to cyber crime); and
- who is most affected (for example, which business areas, which individuals).

2.0 Role of the Working Group

2.1 The role of the Working Group is to direct and undertake the necessary work to improve estimates of both the social and economic costs of cyber crime.

2.2 This includes work to improve the understanding and measurement of prevalence and/or incidence of cyber crime, which will be necessary to improve cost estimates.

2.3 Whilst the financial aspect is important, the remit of the group also includes work to improve understanding of how the wider non-financial harms and impacts of cyber crime are measured.

2.4 Specifically, the Working Group will:

- outline the scope and types of cyber crime that are the highest priority and/or the most viable for developing cost estimates;
- agree on the best available data for developing cost estimates;
- identify and fill any gaps in basic prevalence or incidence data that are required in order to calculate costs;
- develop an agreed model for estimating the costs of cyber crime on a regular and ongoing basis; and
- monitor progress and improve these estimates over time.

2.5 The Working Group will be responsible for:

- setting-up and directing work programmes regarding the eligible work areas (see below);
- producing work plans for both 2014/15 and 2015/16;
- advising on the priority of funding for different projects; and
- monitor progress and deliverables.

3.0 Remit

3.1 The remit of the Working Group incorporates any form of 'cyber crime' as defined by the Serious and Organised Crime Strategy. This includes:

- cyber-dependent crimes (for example, viruses and other malware, hacking, denial of service or distributed denial of service [DDoS] attacks);
- cyber-enabled crimes (for example, cyber-enabled fraud, data theft).

3.2 Exclusions therefore include:

- online crime/abuse where the internet is used as a medium for communication (for example, online harassment, stalking, hate crime); child sexual exploitation;
- online terrorism/extremism;
- high-end cybersecurity attacks (for example, on national infrastructure), or state-sponsored espionage.

These areas are either being covered by work being undertaken by other parts of the Home Office or other parts of the National Cybersecurity Programme. It is, however, important to ensure the work is joined up so that everyone involved can learn from work in other areas.

3.3 Funding for Working Group projects will therefore only be eligible for consideration where bids relate to:

- cyber crime (as defined in the Serious and Organised Crime Strategy);

- measures of prevalence, incidence or scale of any form of cyber crime
- measures of financial cost for any form of cyber crime;
- measures of wider social and economic harms, and other impacts from cyber crime.

3.4 Within these criteria there is more flexibility in terms of specific approaches that could be adopted, shown by the following examples.

- Costs and harms may be explored from either a victim perspective (for example, individuals/public; business; government; society as a whole) or an offender perspective (for example, offender revenue/income from cyber crime).
- Different types of costs and harms are also eligible for exploration (for example, costs in terms of prevention/anticipation of cyber crime; costs as a consequence of cyber crime; costs in response to cyber crime).
- Measures of both current and future types of cyber crime.

4.0 Group membership and structure

4.1 The Working Group will be led by a ‘core’ group of academic, industry and government representatives. They will be responsible for setting the agenda and direction of the work as a whole as well as leading on particular work programmes/themes. The group will be chaired by Professor David Delpy from the Home Office Science Advisory Council.

4.2 ‘Sub-group’ members will be invited to contribute to delivery of projects within the workstreams – there is no specific limit to the number of sub-group members involved.

4.3 Other individuals who are not already involved can be invited to join as sub-group members as various projects develop. Core group leads should consider who else needs to be involved in specific projects as they are planned. Members of the Working Group may invite individuals outside of the Working Group to attend meetings where additional skills, knowledge or expertise is required.

4.4 Representatives from across the Government and law enforcement will help to:

- steer the general direction of the work:
- negotiate access to data or information required for projects; and
- ensure proposed deliverables are timely and relevant.

4.5 Funding is from the National Cybersecurity Programme (NCSP).

5.0 Governance

5.1 The Working Group will sit under the umbrella of the Home Office Science Advisory Council (HOSAC), an independent advisory council that supports the Home Office Chief Scientific Adviser by providing advice on a range of science matters.

Incorporation of the group under HOSAC reflects:

- the importance of the issue to both HOSAC and the Home Office; and
- the importance of applying robust analytical approaches to understanding the problem.

5.2 Although not a formal sub-group, HOSAC may at times request an update regarding the progress of the group. Working Group members should be willing to assist with these updates.

5.3 The workstream leads will report progress (against the work plan) to the full Working Group at each meeting, and seek the Working Group's agreement with its work plan, key decisions and recommendations.

6.0 Deliverables

6.1 Multiple short and longer term projects would run as part of the work programme. Efforts will be made to ensure that there is a spread of interests/areas of coverage in the work programmes, although it may not be possible to cover every aspect of costs. Projects may still be eligible for funding where they fall outside of the core group areas of interest listed. In combination, the findings from these projects will help to provide a better measure prevalence and costs.

6.2 Interim mini-reports with outcomes from these projects will be delivered during the course of the lifespan of the Working Group (i.e. during 2015). These will report back to the whole Working Group.

6.3 At the end of the Working Group (end March 2016) there will be a final report that summarises all project outcomes to provide final assessments of prevalence, costs and harms; and where there may still be gaps in knowledge.

7.0 Ownership of deliverables/intellectual property rights

7.1 The projects will be funded via a grant system, and therefore are not subject to the usual rules of Home Office procured projects. Grant agreements outline details of intellectual property rights, including the points outlined below in 7.2 to 7.4.

7.2 Permission to publish material using the grant shall not be unreasonably withheld from grant recipients. Permission to publish may be withheld if it were to involve the release of data that pose a potential security risk. Particular limitations around publication may also apply around the formal pre-election period ('purdah') from end March to early May 2015.

7.3 Grant recipients must alert the Home Office to any publication plans at least four weeks before publication. The Home Office and the Costs of Cyber crime Working Group must have sight of the planned publication and be given opportunity to comment during this time.

7.4 Express permission to use the Home Office name in connection with any publicity and written material relating to the work funded by the grant must be sought from the Home Office in advance of publication. In the publication, the grant recipient must state that any views expressed in the report are those of the authors and are not necessarily the views or policy of the Home Office (or of the Government more widely).

8.0 Timing

8.1 The Working Group will complete their work by end March 2016. Consideration will be made at this stage as to whether the group should continue (including whether funding is available) or if work is complete. Individual projects and interim findings will be delivered during 2014/15 and 2015/16.

8.2 The Working Group Leads produced a first work plan for November 2014 to March 2015, which was agreed during December 2014. Following funding bids for 2015/16 being agreed, the Working Group produced a work plan for 2015/16 during March 2015. Work plans were reviewed at each meeting.

Appendix 6: Membership of the Costs of Cyber Crime Working Group

Chair:

- Professor Dave Delpy, University College London and Home Office Science Advisory Council

Working Group Members:

- Ruth Davies, Tech UK
- Ali Imanat; Financial Fraud Action UK
- Professor David Pym, University College London
- Professor Steve Furnell, Plymouth University
- Dr Tom Holt, Michigan State University, USA
- Dr Alice Hutchings, Cambridge University
- Professor David Wall, University of Leeds
- Emma Dickens, Cabinet Office
- John Flatley, Office for National Statistics
- Patrick Anderson, National Crime Agency
- Gareth Rees, National Crime Agency
- Dave Fyson, Department for Culture, Media and Sport
- Tom Ryder, National Crime Agency
- Henry Bryers, National Crime Agency
- DI Chris Felton, City of London Police

ISBN: 978-1-78655-392-8

ISSN: 1756-3666