

THE COST OF CYBER CRIME.

A DETICA REPORT IN PARTNERSHIP
WITH THE OFFICE OF CYBER
SECURITY AND INFORMATION
ASSURANCE IN THE CABINET OFFICE.

Executive summary	1
Chapter 1: Introduction	4
Why estimate the cost of cyber crime?	4
Chapter 2: What is cyber crime?	6
What types of cyber crime have we considered?	6
Who are the cyber criminals?	8
What do cyber criminals target?	9
What is the impact of cyber crime?	11
Chapter 3: Study methodology	14
Constraints and assumptions	14
Sources of data on IP theft	14
Our methodology for assessing the impact of IP theft	15
Our methodology for assessing the impact of industrial espionage	16
Chapter 4: Results and analysis	18
Cost to citizens	18
Cost to the Government	19
Cost to businesses	19
Other findings	22
Chapter 5: Conclusions and recommendations	24
The cost of cyber crime is significant and growing	24
The impact of cyber crime is felt most by UK business	24
The UK needs to build a comprehensive picture of cyber crime	24
Annex A: Organisations consulted	25
Annex B: Business sector background	25
About Detica	BC

WHY ESTIMATE THE COST OF CYBER CRIME?

Our society has become almost entirely dependent on the continued availability, accuracy and confidentiality of its Information and Communications Technology (ICT). As well as significant benefits, the technology has enabled old crimes to be committed in new and more subtle ways. In its National Security Strategy, cyber threats are recognised by the Government as one of four 'Tier One' risks to the UK's security.

But estimates of the cost of cyber crime have until now failed to address the breadth of the problem and have not been able to provide a justifiable estimate of economic impact. Therefore, the Office of Cyber Security and Information Assurance (OCSIA) worked in partnership with Detica to look more closely at the cost of cyber crime in the UK and, in particular, to gain a better appreciation of the costs to the UK economy of Intellectual Property (IP) theft and industrial espionage. Further developments of cyber crime policy, strategies and detailed plans thus benefit from greater insight.

WHAT IS CYBER CRIME?

For the purposes of this study, we are using the term 'cyber crime' to mean the illegal activities undertaken by criminals for financial gain. Such activities 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 the Government.

We have not included crimes that lack an over-riding financial motive, or attacks of cyber 'terrorism' or cyber 'warfare'. In our study, we have focused on:

- identity theft and online scams affecting UK citizens;
- IP theft, espionage and extortion targeted at UK businesses; and
- fiscal fraud committed against the Government.

We recognise that the full economic impact of cyber crime goes beyond the direct costs we have been able to estimate in our study, but given the lack of available data and what we believe to be a significant under-reporting of cyber crime, we have had to be pragmatic in our approach.

EXECUTIVE SUMMARY

STUDY METHODOLOGY

To address the complexity of less understood cyber crime, which is the focus of this study, we develop a causal model, relating different cyber crime types to their impact on the UK economy. The model provides a simple framework to assess each type of cyber crime for its various impacts on citizens, businesses and the Government. We use the causal model to map cyber crime types to a number of broad categories of economic impact, which are generally consistent with the types of parameters used in macro-economic models of the UK. We then calculate the magnitude of the costs of cyber crime using three-point estimates (worst-case, most-likely case and best-case scenarios), focusing in particular on IP theft and industrial espionage and its effect on the different industry sectors.

Our assessments are, necessarily, based on estimates and assumptions rather than specific examples of cyber crime, or from data of a classified or commercially-sensitive origin. We have drawn instead on information in the public domain, supplemented by the tremendous knowledge of numerous cyber security, business, law enforcement and economics experts from a range of public and private-sector organisations. We are indebted to all those individuals and organisations who contributed their time and expertise to this study.

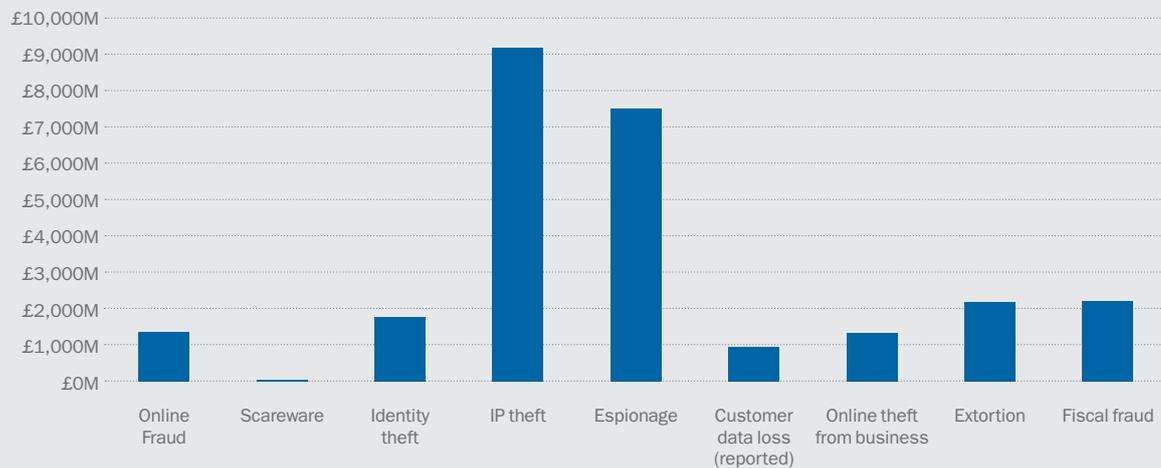
RESULTS AND ANALYSIS

In our most-likely scenario, we estimate the cost of cyber crime to the UK to be £27bn per annum. A significant proportion of this cost comes from the theft of IP from UK businesses, which we estimate at £9.2bn per annum. In all probability, and in line with our worst-case scenarios, the real impact of cyber crime is likely to be much greater.

Although our study shows that cyber crime has a considerable impact on citizens and the Government, the main loser – at a total estimated cost of £21bn – is UK business, which suffers from high levels of intellectual property theft and espionage. Businesses bearing the brunt of cyber crime are providers of software and computer services, financial services, the pharmaceutical and biotech industry, and electronic and electrical equipment suppliers.

Cost of different types of cyber crime to the UK economy

All types of cyber crime



CONCLUSIONS AND RECOMMENDATIONS

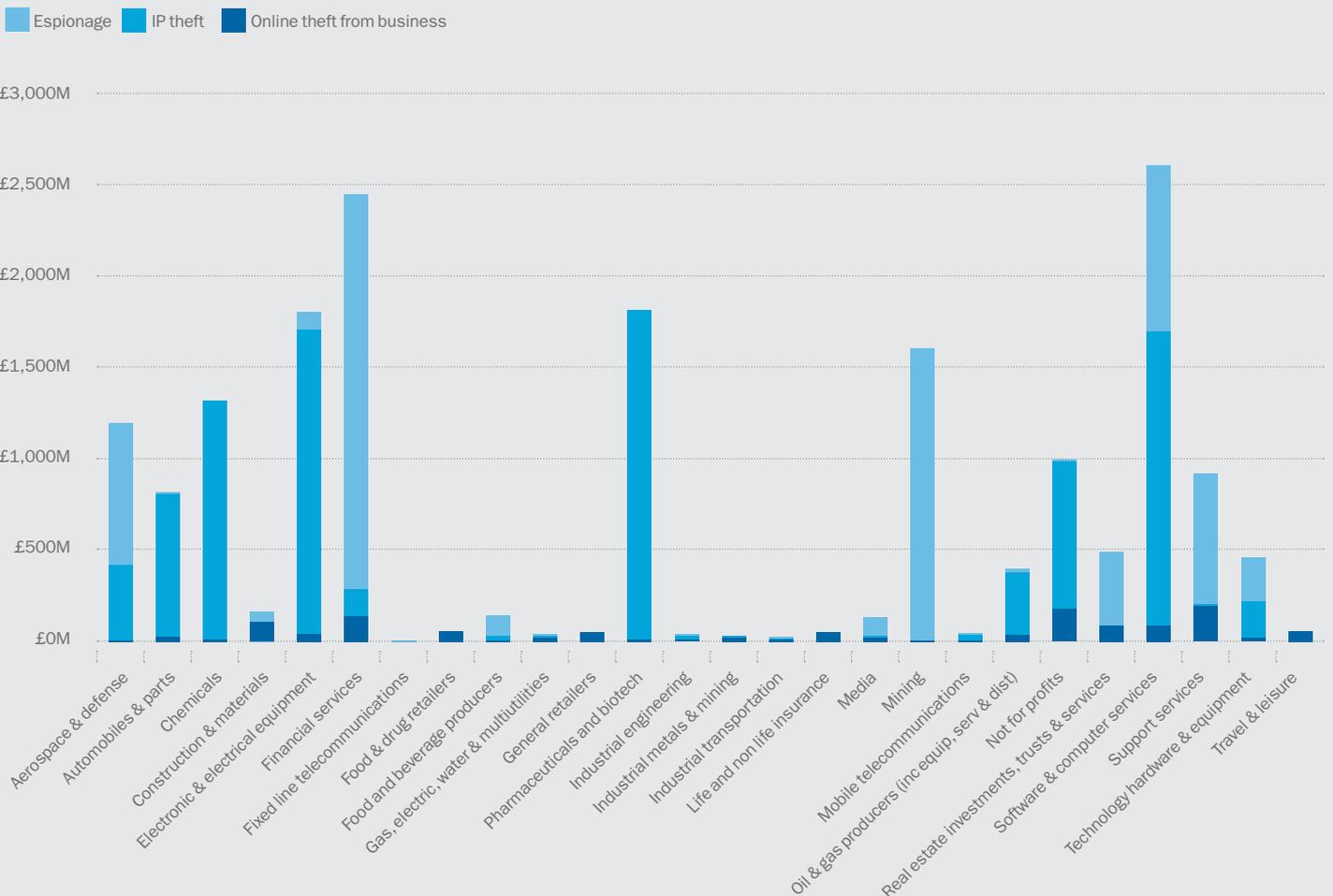
Cyber crime is a national scale issue. The cost to the economy, estimated at £27bn, is significant and likely to be growing. The ease of access to and relative anonymity provided by ICT lowers the risk of being caught while making crimes straightforward to conduct.

The impact of cyber crime does not fall equally across industry sectors. The results also challenge the conventional wisdom that cyber crime is solely a matter of concern for the Government and the Critical National Infrastructure (CNI), indicating that much larger swathes of industry are at risk. The results of this study suggest that businesses need to look again at their defences to determine whether their information is indeed well protected. Without urgent measures to prevent the haemorrhaging of valuable intellectual property, we believe that the cost of cyber crime is likely to rise even further in the future as UK businesses increase their reliance on ICT. However, encouraging companies in all sectors to make investments in improved cyber security, based on improved risk assessments, is likely to considerably reduce the economic impact of cyber crime on the UK.

Although the existence of cyber crime in the UK economy appears endemic, efforts to tackle it seem to be more tactical than strategic. The problem is compounded by the lack of a clear reporting mechanism and the perception that, even if crimes were reported, little can be done. Additional efforts by the Government and businesses to build awareness, share insights and measure cyber crime would allow responses to be targeted more effectively.

£27BN: ESTIMATED COST OF CYBER CRIME IN THE UK.

Cost of different types of cyber crime to UK industry sectors



WHY ESTIMATE THE COST OF CYBER CRIME?

Few areas of our lives remain untouched by the digital revolution. Across the world, there are now nearly two billion internet users and over five billion mobile phone connections; every day, we send 294 billion emails and five billion SMS messages; every minute, we post 35 hours of video to YouTube, 3,000 photos to Flickr and nearly 35,000 'tweets'^{1,2}. Over 91 per cent of UK businesses and 73 per cent of UK households have internet access and £47.2 billion was spent online in the UK alone in 2009³. Our society is now almost entirely dependent on the continued availability, accuracy and confidentiality of its Information and Communications Technology (ICT). We need it for our economic health, for the domestic machinery of government, for national defence and for our day-to-day social and cultural existence.

Despite the technology's obvious benefits, the seeds of criminality planted by the first computer hackers 20 years ago have allowed old crimes to be committed in new and more subtle ways. The information generated by the technology is also a target of considerable interest for individuals, groups, organisations and nation states with more malign intent. And the level of concern expressed by some commentators suggests that cyber crime is a problem of considerable magnitude⁴. In its National Security Strategy⁵, for instance, the UK Government recognised cyber threats as one of four 'Tier One' risks to the UK's security, and subsequently announced a £650m investment in a National Cyber Security Programme.

But, although the fears seem to be well founded, estimates of the impact of cyber crime have until now been no more than 'best guesses'. For example, there is no mandatory reporting regime for citizens, companies or public-sector organisations, which forces them to declare having being the victim of cyber crime and what it has cost them. And the consequential effects of cyber crime may themselves take many weeks, months or even years to play out.

Therefore, the Office of Cyber Security and Information Assurance (OCSIA) worked in partnership with Detica to look more closely at the cost of cyber crime in the UK and, in particular, to gain a better appreciation of the costs to the UK economy of Intellectual Property (IP) theft and industrial espionage. In this study, we were also interested to understand which types of cyber crime have the largest economic impact and the relative risk faced by different industry sectors. Further developments of cyber crime policy, strategies and detailed plans will thus benefit from greater insight.

To address the complexity of less understood cyber crime, which is the focus of this study, we develop a causal model, relating different cyber crime types to their impact on the UK economy. The model provides a simple framework to assess each type of cyber crime for its various impacts on citizens, businesses and the Government. We use the causal model to map cyber crime types to a number of broad categories of economic impact, which are generally consistent with the types of parameters used in macro-economic models of the UK. We then calculate the magnitude of the costs of cyber crime, focusing in particular on IP theft and industrial espionage and its effect on the different industry sectors.

CHAPTER 1 INTRODUCTION

Footnote

- 1 Email and internet statistics from the Pingdom Blog, January 2011 (<http://royal.pingdom.com/2011/01/12/internet-2010-in-numbers/>)
- 2 Mobile statistics from Wireless Intelligence, July 2010 (<http://www.wirelessintelligence.com/analysis/2010/07/global-mobile-connections-surpass-5-billion-milestone/>) and DSLReports.com (<http://www.dslreports.com/shownews/Wireless-Users-Send-5-Billion-SMS-A-Day-107515>), 2010
- 3 "Cyber Security – A new national programme", Emma Downing, House of Commons Library Standard Note SN/SC/5832, 19 January 2011
- 4 For example, see "Industrial espionage: Data out of the door" published in the Financial Times, 1 February 2011
- 5 "A strong Britain in an age of uncertainty", National Security Strategy, October 2010
- 6 "Unsecured Economies: Protecting Vital Information", McAfee, 2009

We have drawn on information in the public domain, supplemented by the tremendous knowledge of numerous cyber security, business, law enforcement and economics experts from a range of public and private-sector organisations. We are indebted to all those individuals and organisations who contributed their time and expertise to this study.

Modelling cybercrime is a complex and difficult exercise. Our assessments are, necessarily, based on assumptions and informed judgements rather than specific examples of cyber crime, or from data of a classified or commercially-sensitive origin. And the implications of cyber crime mean that it is likely to be seriously under-reported. Our results, therefore, should be used as a credible, illustrative guide to the nature of the impacts of cyber crime rather than as accurate and robust estimates of the impacts of cyber crime.

Finally, although Detica has an interest in and capability to defend organisations against many forms of cyber attack, our intent in this study has been solely to examine the cost of cyber crime to the UK economy; it has not been to investigate either the attack methods used by cyber criminals or the origins of such attacks.

BOX 1: FACT NOT FICTION – RECENT EXAMPLES OF CYBER THREATS

Stuxnet worm (July 2010)

The Stuxnet worm (a complex computer code) was used in the first cyber attack specifically targeting industrial control systems. This attack seemed to be directed at Iran, and its nuclear programme. Stuxnet is unprecedented in its design to allow hackers to manipulate real-world equipment without operators knowing¹. The worm targeted Siemens' systems, used in the energy sector to control nuclear and gas infrastructure and also in manufacturing and automotive industries.² Experts estimate that it took five to ten people to work on the Stuxnet worm for six months. The complexity and access to systems involved indicated a highly organised and well-funded project.³ The European Network and Information Security Agency (ENISA) has called it a "paradigm shift" in threat.⁴

Operation Aurora' (December 2009)

Google detected a highly sophisticated and targeted attack on its corporate infrastructure originating from China. The attack was found to have installed malware via email on computers in another 30 companies and Government Agencies.

Large scale fraud (2009/10)

An Essex-based gang, linked to Eastern Europe, was prosecuted for an on-line fraud making £2 million a month by stealing log-in details from 600 UK bank accounts and tricking users into providing additional information. The Police e-Crime Unit, working with the banking sector, detected the fraud which targeted weak security on individual's computers using Zeus Trojan malware (i.e. a malicious computer programme disguised as something else such as an email attachment). The fraud was co-ordinated from a single laptop with sophisticated software available on the internet.⁵

Conficker (2008)

A botnet⁶ on an unprecedented scale has been operating since November 2008 affecting millions of computers worldwide using the Windows operating system.⁷

Distributed Denial of Service Attacks (DDoS): Estonia (2007) and Myanmar (2010) suffered high profile DDoS attacks thought to be politically motivated. In both cases, numerous computers overwhelmed the same target simultaneously. Myanmar was cut off from the Internet after more than 10 days of DDoS attacks which culminated in a massive data flood that overwhelmed the country's infrastructure ahead of the country's general elections. (10) Estonia's financial operations were severely compromised and Government communications networks were reduced to radio for a limited period.⁸

Footnotes

- 1 Symantec briefing, The Stuxnet Worm [on 19 January 2011]
- 2 Stephen Trilling, Senior Vice President, Symantec, Heading off targeted attacks, Symantec CIO Digest, October 2010
- 3 Symantec briefing, The Stuxnet Worm [on 19 January 2011]
- 4 ENISA Press Release, European Agency analysis of 'Stuxnet' malware – a paradigm shift in threats and Critical Infrastructure Protection, 21 October 2010
- 5 Metropolitan Police News Bulletin 1527 Gang sentenced for 'trojan' bank theft scam, 16 November 2010 and High tech crime police quiz 19 people over internet bank scam that netted hackers up to £20m from British accounts, Mail Online, 29 September 2010 (as linked to from Metropolitan Police website).
- 6 A botnet is a group of computers compromised and co-opted by an 'intruder'. A single compromised computer is known as a 'bot'.
- 7 SEC(2010) 1122 final, Council of the European Union, 14436/10 ADD 1, Commission staff working document Impact Assessment: Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, 4 October 2010
- 8 DDoS attacks take out Asian nation: Myanmar fades to black, The Register, 3 November 2010 (9) House of Lords European Union Committee (Sub-Committee F Home Affairs), Fifth Report, Protecting Europe against large scale cyber attacks, Session 2009-10, para 12

For the purposes of this study only, we are using the term 'cyber crime' to mean:

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.

We appreciate that our definition is narrower than that used elsewhere, but we wanted to focus our work on the less understood areas of cyber security that have quantifiable economic consequences. Although we acknowledge the importance of addressing all types of cyber crime in government policy, for the purposes of this study we have excluded:

- cyber bullying;
- distributing indecent material;
- selling counterfeit goods;
- the financial effects of peer-to-peer file-sharing;
- using the profits of cyber crime to fund more conventional crime; and
- other non-financially oriented criminal activity conducted online, such as internet grooming.

We have also made a clear distinction in this study between financially-motivated cyber crime and cyber terrorism or cyber warfare. Of course, all three of these forms of cyber 'attack' can use the same or similar attack methods. However, although both cyber terrorism and cyber warfare can lead to significant direct and indirect economic shocks, the principal difference between them is in the attacker's intent (see below).

WHAT TYPES OF CYBER CRIME HAVE WE CONSIDERED?

There are several distinct 'flavours' of cyber crime, which can impact citizens, businesses, and the UK Government in different ways. All of the following types have cumulative or knock-on effects on the UK's economy as a whole:

- **Identity theft** – cyber criminals obtain personal data from individuals (such as address, date of birth or bank account details) and exploit this online by opening bogus accounts (for example, bank accounts and mortgage applications). In many cases, the victims of identity theft are not even aware of a problem until the impacts become severe.
- **Online scams** – cyber criminals obtain financial or other valuable information by fraudulent means, usually by tricking individuals through scams such as purchase frauds (such as making people pay for goods they do not intend to despatch), 'phishing' (for example, sending bogus money-transfer requests from foreign countries to thousands of e-mail accounts), 'spear phishing' (highly personalised bogus e-mails targeted at a single individual), 'spoofing' (fooling people into entering details into a counterfeit website) and 'pharming' (redirecting website traffic from a legitimate website to a fraudulent website).

Cyber crime

Often re-occurring and common events
Often a mix between individual and organised criminals with potentially some state involvement
Usually the scale of attack is not planned to be critically damaging to the UK economic infrastructure
Primary motive is financial

Cyber terrorism and cyber warfare

Usually highly isolated and unique incidents
Often solely instigated by state-sponsorship
The potential scale of attack is often designed to cause maximum damage to the UK infrastructure
Primary intent is to threaten the UK socio/political infrastructure

Differences between cyber crime and cyber terrorism/ cyber warfare

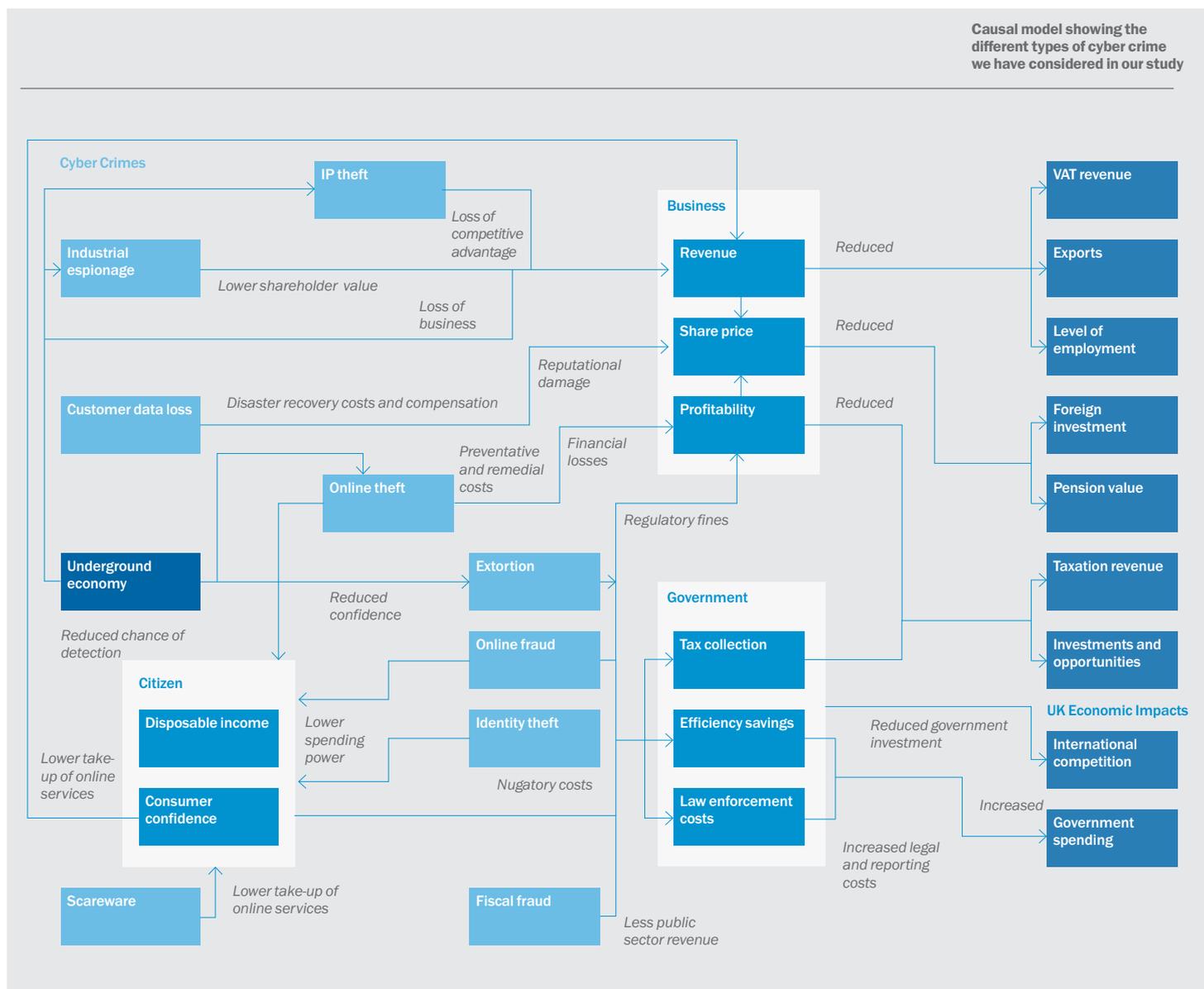
CHAPTER 2 WHAT IS CYBER CRIME?

Footnotes

- 10 Get Safe Online, 'Organised gangs deceive web users into downloading malicious anti-virus software', 15th November 2010
- 11 'Man arrested for £1m online tax fraud', The Register, 4 September 2009.
- 12 'Google probing possible inside help on attack', Reuters January 18 2010.
- 13 'Online Casinos Will Experience Cyber-Extortion During SuperBowl Betting', Internet Business Law Services Kelly O'Connell, IBL Editor, Monday, January 28, 2008.
- 14 For example, US retailer TJX revealed that their customers' personal and financial data had been stolen and could be used to conduct fraudulent transactions.
- 15 For example, see 'Chinese Whispers', Marion Wilkinson, Australian Broadcasting Corporation, April 2010.
- 16 For example, see 'Putting a price on Cyberspying', /Forbes, January 2009.
- 17 For example, see 'Money laundering in cyberspace' BBC, February 2001.

- **Scareware** – cyber criminals mislead individuals into downloading software onto their computers¹⁰ (for example, fake anti-virus software) by using fear tactics or other unethical marketing practices. The software downloaded is often ineffective or may appear to deal with certain types of virus before infecting the computer with its own viruses. Individuals may then have to pay the cyber criminals to remove the viruses and their impacts.
- **Fiscal fraud** – cyber criminals can withhold taxes due or make fraudulent claims for benefits by attacking official online channels (such as online self assessment forms)¹¹. The loss of tax revenue directly affects public-sector spending and the Government’s ability to invest in UK infrastructure.
- **Theft from business** – cyber criminals steal revenue online directly from businesses, which usually involves fraudulently obtaining access and looting company accounts and monetary reserves. In some instances, this cyber criminal activity is greatly assisted by an ‘insider’¹².
- **Extortion** – cyber criminals hold a company to ransom often through deliberate denial of service¹³ (for example, by using malware to flood a company server with erroneous internet traffic) or by manipulating company website links, which can lead to extensive brand damage (for example, by redirecting links for a retailer website to an online pornography website).
- **Customer data loss** – cyber criminals steal sensitive customer data from a company¹⁴ (such as customer financial, medical or criminal record details) with the purpose of selling the data on to other criminal networks or using it themselves for blackmail attempts. For our study, we have not included accidental data loss but only losses from deliberate and technological means.
- **Industrial espionage** – this takes many forms, such as a rival organisation (or associated third party) illegally accessing confidential information to gain competitive or strategic advantage¹⁵ (for example, by finding out a rival’s bid price) or to gain insider knowledge for financial gain (for example, by becoming aware at an early stage of a possible M&A deal). Cyber criminals could use the ‘insider’ information they glean to acquire or sell shares, or, in rare cases, by betting on currency fluctuations.
- **IP theft** – cyber criminals, often sponsored by rival organisations or nation states, steal ideas, designs, product specifications, trade secrets, process information or methodologies¹⁶, which can greatly erode competitive advantage or even the operational or technological advantage prized by nation states over potential adversaries.
- **Money laundering** – cyber criminals use online means to launder the proceeds of criminal acts¹⁷ (for example, through complex, internet-enabled transfers between global or offshore bank accounts). This type of activity is usually associated with organised criminal networks that have a wide or international reach.

We have developed a ‘causal model’ – shown below – to illustrate the interactions between different types of cyber crime, their effect on different stakeholder groups, and the economic impacts they cause.



All of these crimes differ significantly in risk, cost and complexity. And criminals are likely to trade off the risks against the value they perceive the crime can generate. However, compared with other criminal activities, such as drug trafficking or conventional theft, cyber crime in general offers a much more attractive financial proposition, because the rewards are higher, the chances of detection or attribution are lower, there are far fewer barriers to entry and there are no (or few) physical assets or third parties to manage¹⁸ (see below). For these reasons, it is likely that we will see criminal interest in cyber activity continue to flourish¹⁹.

WHO ARE THE CYBER CRIMINALS?

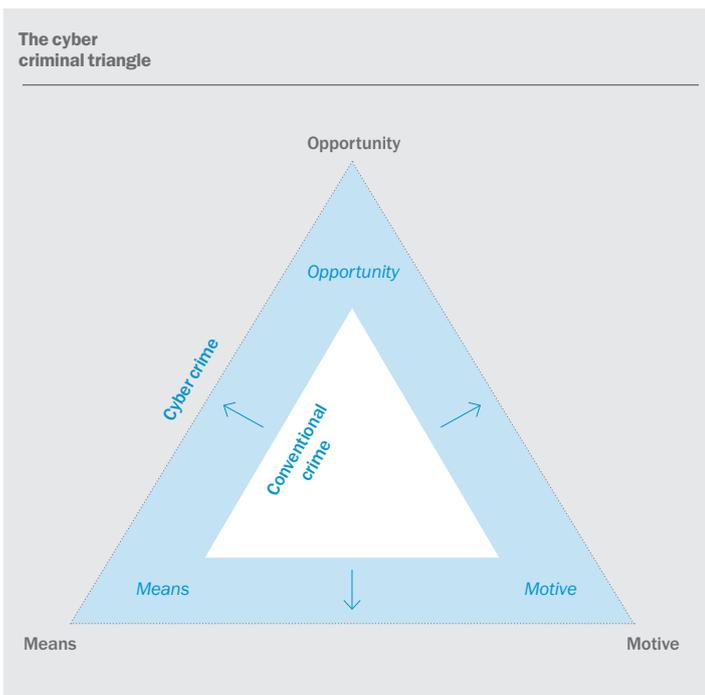
At the highest level, **foreign intelligence services** may have a substantial impact on the UK economy by sponsoring or engaging directly in widespread industrial espionage. This type of cyber criminal tends to be highly organised, with sophisticated techniques and extensive resources²⁰. Particular focus may be given to the theft of IP because this would enable the swift accumulation of knowledge, advancing foreign industries and economies at a fraction of the cost normally needed to develop it. Other priorities for this group could include stealing company-sensitive information to ensure high-value, internationally-competed contracts are won by their preferred bidder.

At the next level, **large organised crime networks** are focusing more of their attention on cyber crime because it offers attractive rewards for minimal investment and low risk²¹. It seems likely that less-sophisticated gangs will focus on online theft from businesses and large-scale online scams. For the more sophisticated networks, with global contacts, industrial espionage can be lucrative, for example, if they combine stolen 'insider' information, such as M&A details, with targeted stock market deals²².

As global competition increases, there is likely to be an increasing risk that **disreputable but legitimate organisations** may engage in cyber crimes such as IP theft or industrial espionage to obtain a rival company's sensitive information. Although it is unlikely that the vast majority of organisations will engage in this type of criminal activity due to the risk it holds for their reputation, some large or under-pressure organisations may believe that the ends justify the means, especially if they are assisted by foreign intelligence services. Alternatively, in an attempt to distance themselves from the crime, disreputable organisations may hire a third party to undertake the cyber crime on their behalf – at a premium price, of course.

At the lower levels, individuals or small groups of **opportunistic cyber criminals** will tend to target UK citizens and vulnerable organisations²³. This group is likely to focus on obtaining revenue through identity fraud, customer-data theft, small-scale online scams, scareware, fiscal fraud and extortion. The level of sophistication shown by cyber criminals in this group depends on their skill and resources, but it is likely that their numbers and influence will grow as cyber crime becomes more lucrative²⁴.

In all cases, however, the UK's continued emphasis on IP development – to sustain our 'knowledge-based' economy²⁵ – means that being able to prevent thefts of IP by cyber criminals is vital.



Footnotes

- 18 Cyber 'Crime has Surpassed Illegal Drug Trafficking as a Criminal Moneymaker', Symantec 2009
- 19 Cybercrime's financial and geographic growth shows no slowdown during the global economic crisis', Marc Fossi, Tech Republic May 2010.
- 20 For example, see 'Canada's Cyber Security Strategy', Vic Toews, Canadian Minister for Public Safety, 2009.
- 21 For example, see 'The Cybercrime Arms Race', Eugene Kaspersky, Securelist, 2008.
- 22 For example, see 'How cyber-crime became a multi-billion-pound industry', The Spectator, June 2007
- 23 For example, see 'Hackers Invade iTunes: Cybercriminals are opportunistic', Peter Chubb, August 2010.
- 24 For example, see 'Cyber crime is a lucrative trade and it's growing', SC Magazine September 3, 2010.
- 25 'The knowledge-based economy: what can the UK do to avoid losing out to the Far East?' BCS Thought Leadership Debate, 16 January 2006

WHAT DO CYBER CRIMINALS TARGET?

Unlike conventional crimes of theft, in which the owner actually loses their physical property, the theft of information by cyber criminals may not result in the loss of anything physical at all. Moreover, the 'theft' can often leave the original data exactly where it was to begin with.

With the exception of the well-understood and documented copyright theft issue, information stolen by cyber criminals often falls into the following categories:

– **Bulk business data** – this often needs to be online to enable efficient transactions to take place, and is usually customer-sensitive (for example, customer addresses or financial details). Any associated data breaches can carry large regulatory penalties as well as substantial reputational damage. Most organisations employ conventional information assurance methods (such as firewalls) to protect this data, and we believe it is targeted mainly by opportunist individual cyber criminals, or small cyber criminal networks. Some types of digital data, once they are stolen, tend to have great longevity – for instance, data containing names, dates of birth, and National Insurance numbers have lifetime durations and cannot be 'reset'. This data will potentially be just as valuable to cyber criminals in the long term as it is now. This is quite distinct from transient data (such as login passwords), which can readily be reset, and are frequently changed on a regular cycle.

– **High-value IP** – different business sectors have different approaches to developing, investing in and exploiting their IP. IP does not necessarily need to be stored online, and usually contains information that has long-term high value to an organisation. While much exists in a tangible form, many other types of IP are intangible – in the form of tacit knowledge and the skills of employees, for example. The types of IP most likely to be stolen by cyber criminals are ideas, designs, methodologies and trade secrets, which exist mostly in tangible form and add considerable value to a competitor. Examples include R&D outputs; product prototypes; documents describing unique business process methodologies or corporate strategies and business decision-making; staff details, including personal information, skill sets and remuneration levels; and descriptions of company capabilities and weaknesses. Any associated data breaches can result in significant damage or compromise to long-term strategy or corporate finances²⁶. Protection for this type of information is often provided by storage on a standalone IT system, complemented by additional physical and personnel security. High-value IP is targeted mainly by foreign intelligence services²⁷, but can also be of interest to high-level organised criminal networks, who can sell the information on to interested third parties²⁸.

– **Tactical corporate information** – frequently this is communicated using online technology but is not necessarily stored online, is low in volume and contains short-term sensitive information (for example, contract bid prices, or share-price sensitive material). Protection for this information typically involves procedural and messaging security implemented at an organisation's senior-management level. It has a high financial impact if it is breached (especially by cyber criminals who operate in the stock market) and is eminently exploitable by cyber criminals if they know how to manipulate or sell this information at the right moment. We believe that this information is targeted mainly by well organised and sophisticated cyber criminal networks, but can also be used by foreign intelligence services to weaken the UK economy²⁹.

When it comes to stealing IP from organisations, there are four ways cyber criminals can obtain what they want. They can:

- **buy it** (in the case of a product), and then reverse-engineer or copy it;
- **carry out a cyber attack**, to obtain the information electronically while remaining outside the organisation's network;
- **carry out an 'insider' attack**, so that the data is stolen by someone authorised to access it from within an organisation;
- **steal it**, by physically breaking-in to office premises or by stealing from employees.

For the purposes of this study, we have defined insider attacks as security breaches associated with employees while cyber attacks are security breaches associated with company technology. Therefore, although we acknowledge that insider attacks can be performed using cyber means, to simplify our model, we have focused our study on external cyber attacks, which tend to go unnoticed and unreported³⁰.

Footnotes

²⁶ For example, see 'The Consumer's Report Card on Data Breach Notification', Ponemon Institute, 2008.

²⁷ GCHQ Press Release, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010

²⁸ For example, see 'Businesses under Cybercrime attack: how to protect your corporate network and data against its impact', Yuval Ben-Itzhak CXO

²⁹ For example, see http://www.us-cert.gov/control_systems/csthreats.html

³⁰ 'E-crime detectives as vital as bobbies on beat', Sir Paul Stephenson, Metropolitan Police Commissioner, Daily Telegraph, October 2010.

HOW EASY IS IT TO EXPLOIT STOLEN IP?

Once they have acquired the IP, cyber criminals will assess its value and how they might be able to exploit it (see *below*).

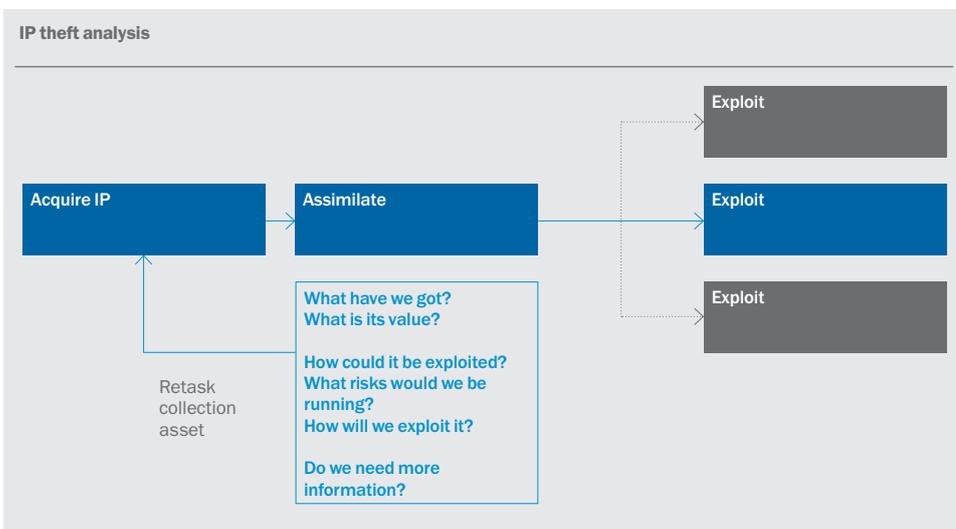
The degree to which the IP can be exploited is likely to depend on the original motives for the theft and a number of other situational factors, such as:

- the importance of time-to-market for the product, organisation, or industry;
- the level of innovation involved and the subsequent value this adds;
- the level of competition and value within an organisation’s industry sector;
- the ability to ‘sell’ stolen IP to third parties via the underground economy;
- the level of interest that the IP has for cyber criminal stakeholders, such as foreign intelligence services.

Once the IP has been acquired by interested cyber criminals or other third parties, it can be exploited in a number of ways, including:

- **producing a direct replica**, which is likely if the IP is not legally protected;
- **producing a similar product using the same concept more quickly**, which is highly dependent on the complexity of the IP;
- **incorporating elements of the IP into an alternative design**, which is highly dependent on how closely the original IP fits the alternative design;
- **becoming inspired to generate new IP**, which is highly situational, and doesn’t guarantee the new IP being successful;
- **selling the IP to a third party**, which is likely if the IP can be commercially exploited by an opportunistic stakeholder;
- **blackmailing the IP-owner by threatening its disclosure**, which is highly dependent on the value of the IP to the organisation.

Ultimately, the overall economic impact of the theft will depend on the market size for the stolen IP and other market forces, which will drive the IP price. Given this wide range of possible mechanisms, the degree to which stolen IP can be exploited depends on the nature and inherent complexity of the industry sector.



WHAT OTHER MEASURES CAN BE USED TO PROTECT IP?

As well as measures to improve cyber security, organisations can also protect their information, to some extent, by legal means such as patents, trademarks and non-disclosure agreements. While these measures provide some assurance for UK organisations that their information will not be unfairly and unlawfully exploited, some of the legal protections may be limited in their effectiveness. For example, certain types of IP such as computer software or unique business processes, cannot always be patented in the UK yet they remain highly valued and coveted by organisations worldwide³¹. Even when the IP can be patented or registered, the investment required to maintain the protections may be prohibitive³² and the protections themselves may force unwanted disclosure. For example, patent applications, which are available in the public-domain, can reveal not only elements of the IP that the company would have preferred to keep secret but also their market intentions³³. Furthermore, the patent application process can be lengthy, particularly where there may be existing applications or patents for similar products³⁴.

Once a patent has been approved, subsequent enforcement activities may be ineffectual, especially in international markets. In some cases, and usually with considerable investment in marketing, organisations may benefit from their IP becoming an industry standard (such as VHS, DVD-Video or BlueRay), but this is by no means guaranteed.

The challenges associated with some of these legal protections have led to many companies resorting to secrecy, with non-disclosure agreements or similar provisions in their contracts of employment. The danger with this approach is that cyber attacks become particularly threatening, especially when the IP is accessible from online computer systems.

WHAT IS THE IMPACT OF CYBER CRIME?

We have adapted the methodology used by the Home Office in their 2001 report on the economic impact of crime in the UK³⁵ to define the following types of cost associated with cyber crime:

- **costs in anticipation of cyber crime**, which include individual and organisational security measures (such as installing physical and virtual protection such as antiviral software), insurance costs and costs associated with gaining compliance to required IT standards (for example the Payment Card Industry Data Security Standard, PCI DSS);
- **costs as a consequence of cyber crime**, which take into account direct losses to individuals and companies (including business continuity and disaster recovery response costs), and indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness;
- **costs in response to cyber crime**, such as compensation payments to victims of identity theft, regulatory fines from industry bodies and indirect costs associated with legal or forensic issues;
- **indirect costs associated with cyber crime**, which include such factors as reputational damage to organisations, loss of confidence in cyber transactions by individuals and businesses, reduced public sector revenues and the expansion of the underground economy.

We have used these definitions to examine more closely the impact of cyber crime on the principal stakeholder groups – citizens, businesses and the Government – as well as exploring the macro-economic impacts.

IMPACT ON CITIZENS

Citizens can help themselves reduce the impact of cyber crime by ensuring that they take a number of sensible precautions to stay safe online, such as installing a firewall, regularly patching or updating software applications and using legitimate anti-virus software. They can also take out specialist insurance to protect against the impact of identity theft. These costs, in anticipation of cyber crime, have not been included in our study.

No defences are foolproof, though, and even well-prepared citizens are likely to suffer a range of costs as a consequence of and in responding to cyber crime: victims of identity theft can be left to pick up the tab for loans taken out under their name by cyber criminals; victims of online scams can find their credit card details are used by cyber criminals to purchase goods or services; victims of phishing scams can be tricked into revealing passwords, PIN numbers and other sensitive financial information that cyber criminals can subsequently sell or exploit. Alternatively, citizens may be compelled into purchasing defective software as a result of receiving or inadvertently downloading scareware.

The wide-ranging and large-scale nature of many of these individual cyber crimes means that their aggregate effect can be detrimental to the UK economy.

Furthermore, indirect macroeconomic effects could occur as a result of cyber crimes committed on UK citizens, for example, from a loss of confidence in services such as online banking (although anecdotal evidence seems to suggest this isn't the case³⁶), or because they subsequently spend less, which has a knock-on effect on the retail industry.

Footnotes

31 UK Intellectual Property Office

32 For example, see <http://www.ip-holdings.com/patent-enforcement>

33 For example, see 'Using Patents in Competitive Intelligence', Gregory J. Kirsch and Charley F. Brown, SCIP

34 For example, see 'The Patent Application Process in the UK', By Waheedan Jarwalla

35 Home Office methodology described in 'The economic and social costs of crime', Home Office Research Study 217, 2001

36 Closing In on Bank Customer Churn', CRM Magazine, May 2007

IMPACT ON BUSINESSES

In anticipation of coming under attack by cyber criminals, many UK businesses are investing in stronger physical security, such as 'air-gapped' networks, advanced intruder detection hardware, or training initiatives to increase their employees' awareness of cyber crime. These initiatives are particularly important for IP-rich business sectors, such as the pharmaceutical and biotechnology sectors, which invest heavily in R&D and rely on it to create market advantage in a fiercely competitive global industry. As before, though, these costs have not been assessed as part of our study because they are 'business-as-usual' costs that would have been incurred anyway.

Businesses are likely to incur significant direct costs as a consequence of cyber crime, however. The most obvious of these is from online theft. Extortion may lead to less direct costs, such as the loss of business incurred as a result of denial of service attacks or by manipulation of corporate websites. The theft of sensitive information or IP can significantly erode competitive advantage in the marketplace if it is subsequently exploited by another party.

These costs could potentially impact any of the six functions in the business value chain³⁷:

- R&D, because companies are less likely to invest;
- design of products, services, or processes, because companies are less willing to turn new ideas into products;
- production, because companies want to reduce costs;
- marketing and sales, because companies want to cut expenditure to reduce their attractiveness to the underground economy;
- distribution, because companies are affected by reduced demand for exports;
- customer service, because companies have less money to spend on their customers.

Costs associated with cyber crime for organisations include implementing their business continuity and disaster recovery plans, which can divert personnel and resources away from business-as-usual activities, good will and compensation payments to customers affected by online scams and identity theft, regulatory penalties for customer data breaches, and 'clean-up' consultancy costs associated with legal and forensic issues.

Indirect costs could arise from share-price manipulation, enabled by sophisticated industrial espionage, as well as the attrition of UK industry influence overseas as a result of IP theft.

Although there is no legal obligation under the Data Protection Act (1998) on data controllers to report breaches of security that result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches – whether by accidental loss or from cyber criminal activity – should be brought to the attention of his Office³⁸. However, companies can only declare the losses if they are aware of them in the first place – and cyber criminals are increasingly adept at covering their tracks. Moreover, in light of the substantial financial penalties that could be levied and the potential damage to their reputations, some organisations may also attempt to conceal the loss from their customers and the regulator. We have assumed, therefore, that losses of customer data by UK organisations are running significantly higher than the current statistics would suggest.

IP theft and customer-data loss can also increase the cost to businesses even if the data is not actually exploited by cyber criminals. However, costs incurred as a result of reputational damage, for example, are particularly hard to measure and will affect different organisations in different ways. Some cyber crimes may not significantly affect a company's reputation at all, for instance, particularly if customers have a limited choice of alternative suppliers.

The knock-on effects of IP theft or industrial espionage on UK companies include:

- reduced turnover through direct loss of business;
- reduced profitability by losing first-to-market advantage and increasing price-competition;
- reputational damage caused by disclosure of the theft and arrival on the market of counterfeit goods;
- reduction in share price, which may be particularly acute if the company also happens to be an acquisition target;
- loss of competitive advantage, which may be more apparent in overseas markets;
- additional costs incurred through attempts to protect future IP;
- opportunity costs, as the company becomes less willing to invest;
- redundancies as R&D facilities and product lines decrease in capacity or are closed;
- company failures, particularly if the theft has occurred from Small-to-Medium Enterprise (SME) reliant upon IP-enabled trade sales;
- reduction in investment from overseas.

As before, while the costs to individual businesses are by no means insignificant, the aggregate cost of cyber crime on UK businesses overall is likely to be of considerable economic impact.

IMPACT ON GOVERNMENT

The Government and public-sector bodies spend significant sums of money on security to reduce the impact of crime in the UK. These costs, which include the annual expenditure of the Police Central E-crime Unit³⁹, for example, already factor in an increasing focus on cyber crime. They are not included in our study, though, because these resources also provide benefits in combating many other types of crime and insecurity.

However, direct costs in responding specifically to cyber crime include lost corporation and personal taxation revenue as a result of fiscal fraud, as well as the cost of fines levied for personal data breaches.

Finally, there are significant indirect costs for the UK Government, particularly because increasing levels of cyber crime could limit the scale of efficiency savings made by moving more government services online. Furthermore, with cyber crime affecting tax revenues and diminishing the confidence of overseas investors, the UK's continued economic growth may suffer.

Footnotes

37 Value Reference Model (VRM) developed by the trade consortia Value Chain Group.

38 'Notification of Data Security Breaches to the Information Commissioner's Office', ICO

39 The current PCEU budget is £2.3M per year, revealed in a Computing.co.uk interview with the Head of the PCEU on 11 November 2010.

40 Symantec Report on the Underground Economy July 07–June 08.

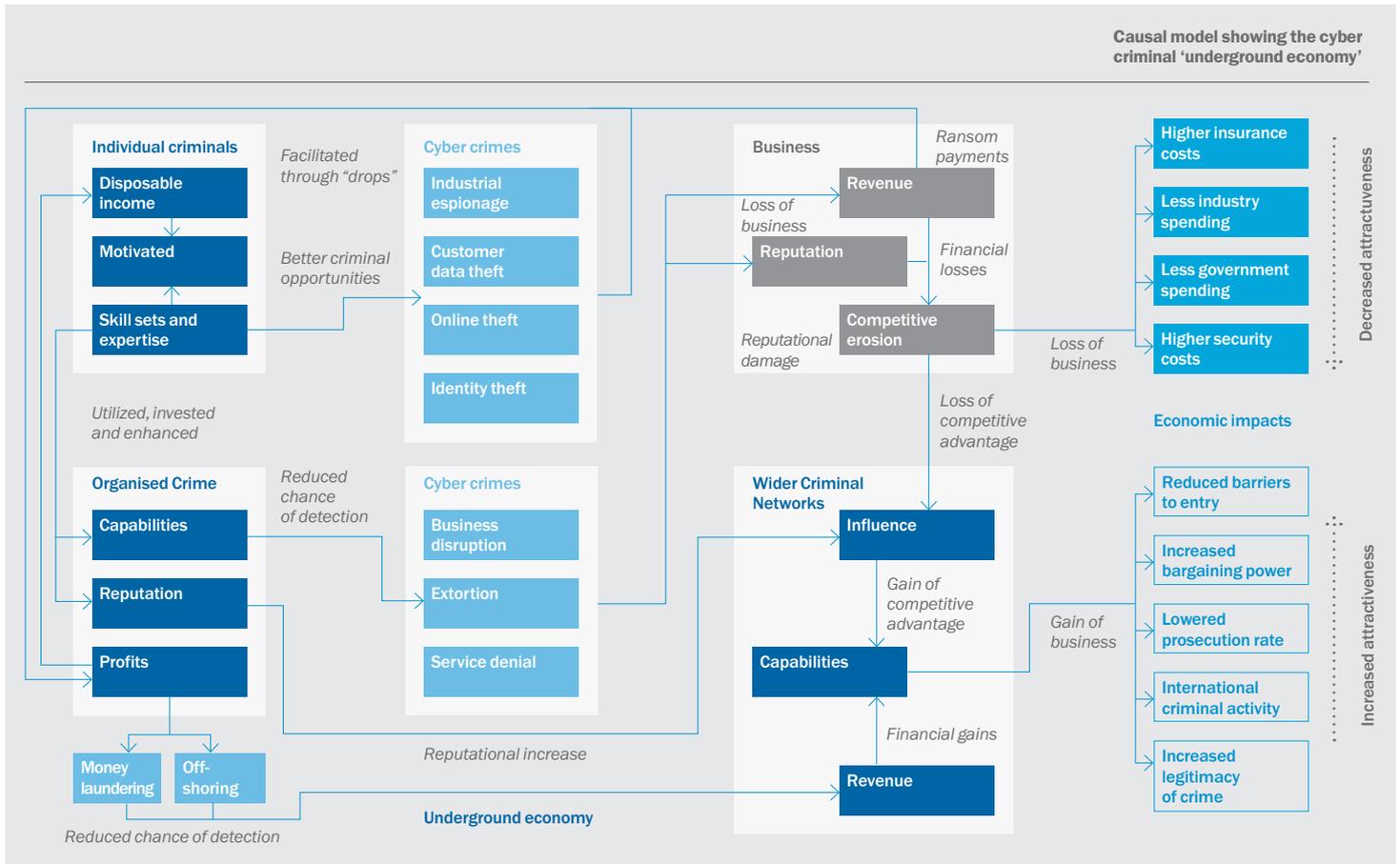
41 'Cybercrime Growth Accelerating' by Keith Ferrell, Information Week, August 2010

MACROECONOMIC EFFECTS

Our model shows that different stakeholder groups are affected by different economic impacts. The impacts of cyber crime are also interdependent. For example, if citizens have less money in their pockets, they may spend less, therefore exacerbating revenue losses from business. For the UK Government, widespread cyber crime may lead to stronger international competition from overseas businesses, significantly reduced revenues from taxes and VAT receipts, and limited scope for spending to improve the UK's infrastructure.

Perhaps one of the biggest significant long term threats is the rise of the so-called 'underground economy'⁴⁰ (for example, see below), which provides a viable economic growth model in itself, and can lead to talented individuals being drawn away from the legal economy if they are unemployed or if it is viewed as a more attractive alternative. As technology enables individual criminality to morph into something less opportunistic, more organised and ultimately more successful, criminal gangs from further afield, financed by global networks or by hostile foreign states, may be attracted to the UK.

As the criminality increases in sophistication and profitability, it is likely to have an ever higher cumulative impact⁴¹, which may cause the legitimate mainstream UK economy to decline in revenue and influence.



To address the complexity of cyber crime, our study developed a causal model, relating different cyber crime types to their impact on the UK economy. The model provided a simple framework to assess each type of cyber crime for its various impacts on citizens, businesses and the Government. We used the causal model to map cyber crime types to a number of broad categories of economic impact, which are generally consistent with the types of parameters used in macro-economic models of the UK. We then calculated the magnitude of the costs of cyber crime, focusing in particular on IP theft and industrial espionage and its effect on the different industry sectors.

CONSTRAINTS AND ASSUMPTIONS

Our study has focused on the costs as a consequence of cyber crime, and has included some additional costs in response to cyber crime where these can be realistically estimated. However, because the situation is inherently complex, we have had to apply a number of constraints to our estimating methodology. These are:

- The impact has been measured as a ‘snapshot’, using the economic situation of 2010 as a baseline. We have not attempted to predict economic impacts for 2011 or beyond because market conditions still remain fluid and a very large number of variables can affect our estimates.
- Because economic data for UK industry sectors and citizens varies considerably depending on its source and context, we have based our estimates wherever possible on economic data provided by official government bodies, such as the Department for Business, Innovation and Skills and the ‘Blue Book 2010’⁴². Although we have used the most up-to-date information, unfortunately it has not always been possible to obtain 2010 data; therefore our estimates have been based on the most contemporary data available and applied as if they were 2010 data.
- Although certain indirect economic impacts can be attributed to cyber criminal activity, we have not included those which exhibit a high degree of situational complexity. For example, we have excluded the short-term fluctuations in a company’s share price caused by theft of customer data. Our attempts to measure this sort of impact would be made challenging because such fluctuations would depend on the prevailing market conditions at the time of the theft and a number of other factors specific to the individual company affected.

- We have excluded costs in anticipation of cyber crime, such as insurance costs and the costs of purchasing anti-virus software, because these are likely to be factored into normal day-to-day expenditure for the Government, businesses and individuals.

In general, our approach to estimating economic impacts is conservative where there is a high degree of uncertainty – as there is in many cases – caused by a lack of data, particular sensitivities or where we know cyber crime is going under-reported⁴³. For most of these areas, we have used three-point estimates – worst case, best case and most likely case – to allow for sensitivity and scenario analysis⁴⁴. Accordingly, we cannot provide definitive estimates of economic impacts for cyber crime in every case and for every industry. Rather, one of our primary aims was to provide a framework for future estimates, which can be updated as more accurate information is obtained through further study and analysis.

SOURCES OF DATA ON IP THEFT

Our study has identified two methods for calculating the costs to the UK economy of IP theft through cyber crime.

The first method used the total R&D expenditure for each UK industry sector as a starting point⁴⁵. The expected return on investment as a percentage for this R&D spend was estimated, which created an overall market value for the IP. This value recognises that IP theft does not just lead to short-term losses from R&D spend, but also to future losses from the value that industry sectors would wish to recoup from their initial expenditure.

The second method started with the total cash flow for each UK industry sector, and then estimated the fraction that was attributable to IP within the industry. This calculated the subsequent economic value.

CHAPTER 3 STUDY METHODOLOGY

Footnotes

⁴² UK National Accounts Blue Book 2010, Office for Government Statistics

⁴³ ‘Law of Electronic Commerce’ by Jane Winn and Benjamin Wright.

⁴⁴ ‘Three point estimates and quantitative risk analysis’, MOD 2007

⁴⁵ Department for Business, Innovation and Skills, 2010, R&D Scoreboard and Office of National Statistics, 2008, Expenditure on R&D performed in UK businesses.

⁴⁶ For example, see ‘The Business of Cybercrime - A Complex Business Model’, A Trend Micro White Paper, January 2010

⁴⁷ UK National Accounts Blue Book 2010, Office for Government Statistics

Once the economic value of the IP had been derived from both methods, estimates were made of the probability of cyber theft for each industry sector using three point estimates, with the subsequent IP exploitability and revenue impact also calculated as a percentage. This enabled us to assess the economic impact of IP theft on both the basis of R&D spend and the overall economic value of IP.

OUR METHODOLOGY FOR ASSESSING THE IMPACT OF IP THEFT

In developing our methodology for measuring the impact of IP theft, we have made assumptions about:

- the total amount of R&D spend in each UK business sector (using up-to-date and credible data where it is available);
- the average estimated return on investment that each UK business sector would expect from its R&D spend (to estimate the true value of the IP and not just the current market worth);
- the average estimated level of IP 'exploitability' for cyber criminals (recognising that not all IP can be easily exploited);
- the level of economic impact that IP exploitation would have on the UK economy (recognising that, even though it may be exploited, stolen IP does not necessarily lose all of its residual value).

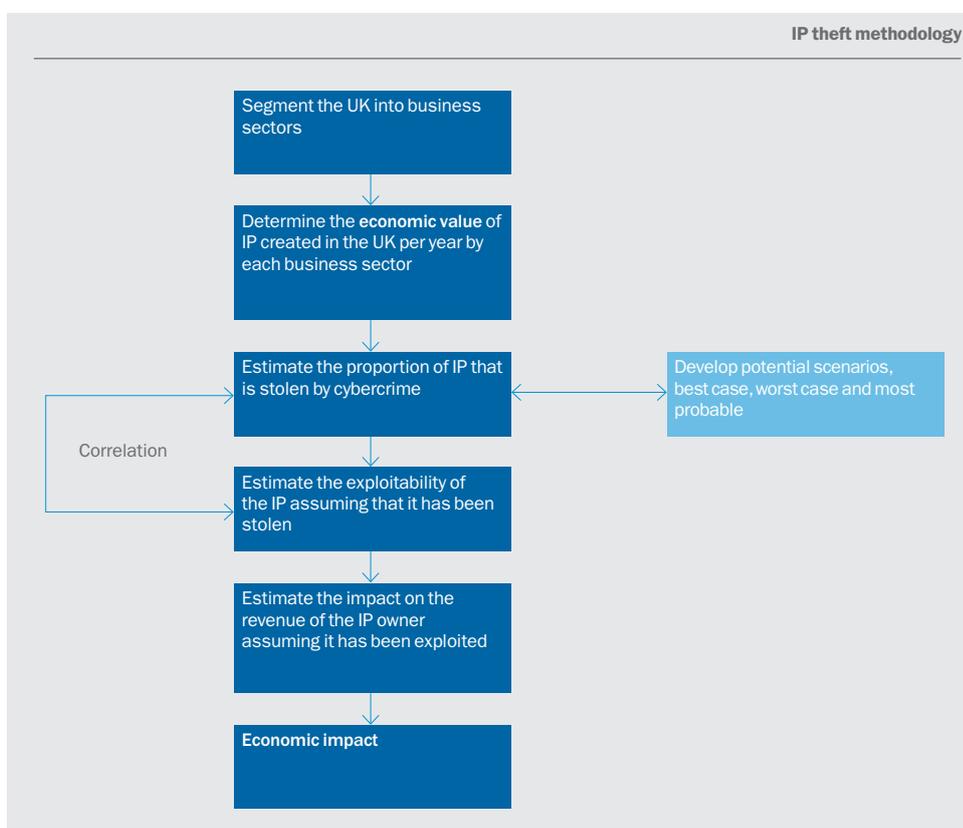
In the absence of robust estimates for actual levels of IP theft, our methodology assumes that the 'business model' cyber criminals adhere to for IP theft follows the same principles of any other type of business⁴⁶: the desire to maximise financial gain and minimise business risk.

For IP theft by cyber criminals, our methodology attempts to determine the means, motive and opportunities presented to potential attackers. It recognises that the nature of IP generated in different business sectors is different and has different levels of exploitability and economic impact if it is stolen.

Therefore, the method used by our study to calculate the costs to the UK economy of IP theft through cyber crime started with the value added to the UK economy by each industry sector as given in the Blue Book⁴⁷. We then estimated the fraction that was attributable to IP within the industry. This calculated the subsequent economic value.

Once the economic value of the IP had been derived, estimates were made of the probability of cyber theft for each industry sector using three point estimates, with the subsequent IP exploitability and revenue impact also estimated as a percentage.

The results give an estimate of the value lost to the economy due to IP theft across the different industry sectors.



The methodology is illustrated above:

Given the number of variables and lack of 'official' data, our methodology uses a scenario-based approach, which establishes three-point estimates to determine the range of uncertainty. Using this approach, we have identified:

- **The best-case scenario:** IP thefts by cyber attack are not widely reported because, although they may be technically possible, they are not widespread. Therefore a very small amount of IP is actually stolen.
- **The worst-case scenario:** The sophistication of and resources available to cyber criminals, coupled with the vulnerability many businesses have to cyber attack, means that most IP worth stealing is actually stolen. The logic of this position is that if cyber criminals have the means, motive and opportunity they will use it for financial gain. In this scenario, the economic impact is limited by the ability of the cyber criminal to exploit the IP effectively rather than to acquire it.
- **The most likely scenario:** Theft of IP by cyber criminals can occur but it needs to guarantee a big return. The level of IP theft within a business sector is therefore determined by the level of motivation of the criminal to attack specific targets, which means that some business sectors are significantly more attractive than others.

This report assumes that there are two possible models of IP theft used by cyber criminals. The first model would see cyber criminals targeting selected companies to acquire specific information that they know can be exploited effectively. In this model, the IP is targeted explicitly, possibly 'to-order' if the attacker is working on behalf of an otherwise legitimate business. The second model would see cyber criminals attempting to obtain IP in bulk from as many companies as possible and then assessing it to determine whether to exploit it, if at all. We believe it is likely that both models are occurring in parallel.

However, the proportion of IP actually stolen cannot at present be measured with any degree of confidence. Our methodology makes the assumption that the level of IP theft is proportional to the level of motivation that cyber criminals have in acquiring it. We have further assumed that their level of motivation is affected by the following factors:

- Their ability to obtain the IP using alternative means, for example by reverse-engineering a legitimately-acquired sample, which would reduce or indeed remove their motivation for a cyber-attack.
- The importance they place on time-to-market in the sector, which increases the motivation for a cyber attack if time is more of the essence.
- The level of innovation typically present in the IP within the sector. A high level of innovation would make the IP intrinsically more value to cybercriminals, hence a higher degree of motivation.
- The size of the market that exploitation of the IP will allow them to address.
- The level of security awareness within the sector and the deployment of security countermeasures by targeted companies. Although this may be a factor in reducing the success rate of IP thefts, we do not think that increased levels of security will necessarily reduce the level of motivation for an attack where the returns are sizeable. Instead, it may motivate the cyber criminal to use even more sophisticated means.

OUR METHODOLOGY FOR ASSESSING THE IMPACT OF INDUSTRIAL ESPIONAGE

It is very hard to determine what proportion of industrial espionage is due to cyber crime. For example, is company-sensitive information stolen through hacking into a company's systems or by the physical theft of printed documents? Is unauthorised access to company sensitive information granted by leaked documents e-mailed from an insider or by a deliberate cyber attack originating from outside the company? In many cases, we believe that companies may be completely unaware that they are the victims of industrial espionage. Like IP theft, this is likely to lead to crimes being under-reported and underestimated.

In developing the methodology for estimating the impact of industrial espionage, we have made assumptions about:

- the value added to the UK economy by each UK business sector using up-to-date and credible data where available⁴⁸;
- the average proportion of open tender contracts placed in each UK business sector, the likelihood of UK organisations winning at least one of these contracts, and the level of exploitability for rival organisations should they gain access to sensitive contract documents;
- the total value of M&A activity for each UK business sector using up-to-date and credible data where available⁴⁹;
- the expected rate of return on investment in shares for targets of M&A activity, short selling and currency-price fluctuations, and the level of exploitability of commercially-sensitive information (to assess impacts from illegal investment in shares for target organisations, the impact from illegal investment in short selling and the impact of market fluctuations respectively).

In line with IP theft by cyber criminals, our methodology has attempted to determine the means, motive and opportunities presented to potential attackers. It recognises that the nature of industrial espionage in different business sectors is different and has different levels of exploitability and economic impact if it is stolen.

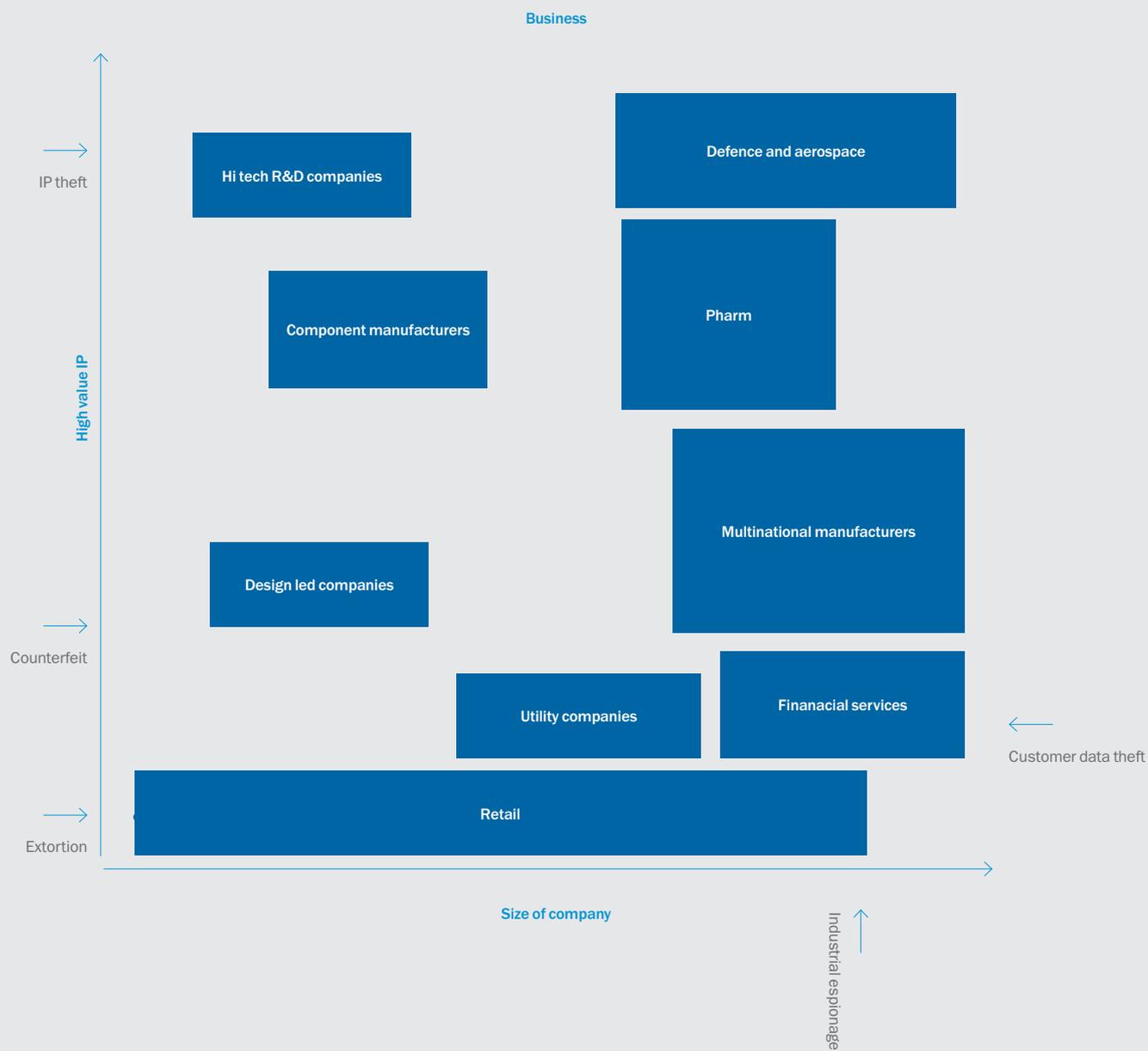
It is our belief that it is more likely that cyber criminals will target organisations for espionage based on size and perceived revenue rather than the business sector that they operate in, as illustrated opposite).

**IN MANY CASES,
WE BELIEVE THAT
COMPANIES MAY
BE COMPLETELY
UNAWARE THAT THEY
ARE THE VICTIMS
OF INDUSTRIAL
ESPIONAGE.**

Footnotes

⁴⁸ UK National Accounts Blue Book 2010, Office for Government Statistics

⁴⁹ PKF, 2010. Deal Drivers UK



The results of our study provide one of the first detailed assessments of the cost of cyber crime to the UK economy, which, in our most-likely scenario, we estimate to be £27bn per annum. A significant proportion of this cost comes from the theft of IP from UK businesses, which we estimate at £9.2bn per annum. Our results challenge the conventional wisdom that cyber crime is solely a matter of concern for the Government and Critical National Infrastructure (CNI), indicating that much larger swathes of industry are at risk.

This section describes in more detail the results of our study for different stakeholders and how the cost of each type of cyber crime was calculated.

COST TO CITIZENS

We considered three types of cyber crime that impact on individual citizens:

- identity theft;
- online scams;
- scareware.

The impact of identity theft was estimated in two ways, based on information published by CIFAS⁵⁰, in particular:

- the number of reported incidents was multiplied by the average cost of an incident and a further estimate made for the level of under-reporting (we estimated that only one in 15 incidents are reported);
- the number of UK citizens with internet access was multiplied by the probability that they became a victim of identity theft, modified by an estimate of the proportion of these crimes being conducted online (which we conservatively estimated at 25 per cent).

Both methods of calculation provided similar answers, with an average of £1.7bn per annum, which compares well with the results of other studies by CIFAS, which also made an estimate of £1.7bn per annum⁵¹, and the IFSC, which reported a figure of £1.2bn⁵² per annum.

We used a similar approach to estimate the cost of online scams, in which we took the total number of UK citizens who have shopped online⁵³ and multiplied this by the estimated percentage who may have experienced fraud⁵⁴ and the average cost of the fraud⁵⁵. This gave an estimate of the total cost of online scams of £1.4bn.

Finally, the costs of scareware and fake anti-virus were calculated from information published by Symantec⁵⁶ on the probability of such an attack and its average cost. The resulting figure of £30m was by far the lowest for any type of cyber crime, but it has been identified as an area of growth⁵⁷.

The table below presents a summary of the results of the cost of cyber crimes to individual citizens.

Cyber crime	Economic impact
Identity theft	£1.7bn
Online fraud	£1.4bn
Scareware and fake AV	£30m
Cost of cyber crime to UK citizens	

Therefore, our overall the estimate for the economic cost of cyber crime to UK citizens is £3.1bn per annum.

CHAPTER 4 RESULTS AND ANALYSIS

Footnotes

- 50 CIFAS, 2006. Identity Fraud – What About The Victim?
 51 Ibid
 52 'New Estimate of Cost of Identity Fraud to the UK Economy', Identity Fraud Steering Group (IFSC), 2008.
 53 Source: Get Safe Online.
 54 Ibid
 55 Ibid
 56 Symantec, 2009. Report on Rogue Security Software
 57 'Growth of 'scareware' is frightening', by Ced Kurtz, Pittsburgh Post-Gazette July 11, 2010.

COST TO THE GOVERNMENT

We used two approaches to assess the cost of fiscal fraud by cyber criminals to the Government.

The first approach took information from the NFA Annual Fraud Indicator⁵⁸, which estimates the total cost of:

- tax fraud;
- benefits fraud;
- local-government fraud;
- central government-fraud;
- NHS fraud;
- pension fraud.

The total cost was combined with an estimate from NFA⁵⁹ on the proportion of fraud that is attributable to ‘criminal attacks’. For the purposes of our study, we assumed that all of these ‘attacks’ were cyber attacks⁶⁰.

This gave an overall figure for fiscal fraud by cyber criminals of £2.2bn. However, although we have used the most up-to-date information available, we believe it may be underestimating the total level of cyber crime against government systems and, therefore, further work in this specific area may be of value.

COST TO BUSINESSES

Our study looked at the cost to business of the following types of cyber crime:

- IP theft;
- industrial espionage;
- customer data-loss (reported);
- online theft;
- extortion.

The results for each of these types of cyber crime are provided in the following sub-sections.

IP THEFT

In Chapter 2 of this report, we describe the issue of IP theft in some detail, including the impact on different business sectors. Because we believe the level of IP theft will vary by sector, individual assumptions were made for:

- the probability of IP theft in the sector;
- the level of exploitability of the IP in the sector;
- the revenue impact on the company if a rival is able to exploit the IP.

Our approach produced three-point estimates for the economic value of IP by taking published figures for the cash flow per year in each sector and estimating the fraction attributable to IP.

The results are provided below:

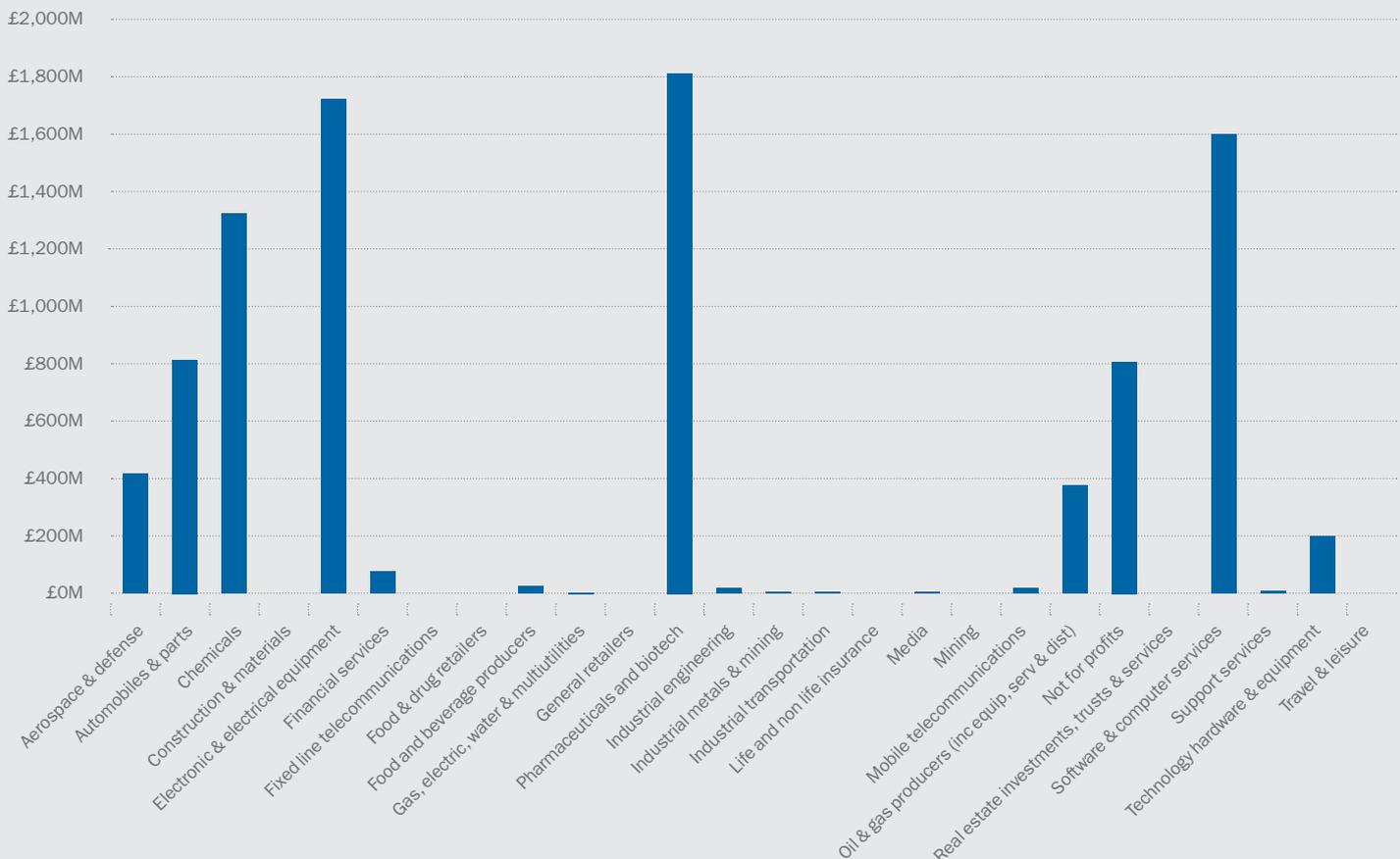
Our results for the most-likely scenarios show that the following business sectors are most likely to be impacted by IP theft⁶¹:

- **aerospace and defence** – £0.4bn per annum – which is likely to be due to the high likelihood of companies in this sector being subject to a cyber attack and the relative exploitability of their IP;
- **chemicals** – £1.3bn per annum – which is likely to be due to the high volumes of IP generated in this sector and the relative ease with which it can be exploited;
- **electronic and electrical equipment** – £1.7bn per annum – which is likely to be due to the relative ease with which the IP generated by companies in this sector can be exploited;
- **software and computer services** – £1.6bn per annum – which is likely to be due to the relative ease with which the IP generated by companies in this sector can be exploited;
- **healthcare, pharmaceutical and biotechnology** – £1.8bn per annum – which is likely to be due to the high volumes of IP generated by companies in this sector.

We note that, although none of the other business sectors are likely to be entirely immune from IP theft, the impact of cyber attacks here is likely to be much smaller due to the relatively low volumes of IP generated in these sectors.

Annual costs by business sector of IP theft by cyber criminals

IP theft – most likely economic impact by business sector



Footnotes

58 National Fraud Authority, 2010, Annual Fraud Indicator

59 Ibid

60 This assumption was made due to the high volume of financial transactions made using online means.

61 Assumptions are based on anecdotal evidence and information from BIS innovation.gov.uk

INDUSTRIAL ESPIONAGE

A more detailed discussion of the impact of espionage has been given in Chapter 2. During our study, we made three-point estimates of the costs to the UK of:

- **The loss of competition-sensitive information** – we estimated the proportion of a sector’s annual value-added to the UK economy that is dependent on large-scale tendering competitions, and multiplied this by estimates for the probability that any of these would be subject to cyber attacks and the resultant exploitability of the stolen information.
- **Information on mergers and acquisitions** – we estimated costs by taking the total value of mergers and acquisitions for each business sector in the last year and multiplying these by estimates for the probability that any of these would have been subject to cyber attack, the exploitability of the information and the maximum illegal return that could be generated without the exploitation being detected. Separate calculations were made for cybercriminals being able to manipulate the share price of the organisation through ‘short selling’ or, in the case of exceptionally large mergers, benefiting from exchange rate fluctuations.

Our total estimate for industrial espionage is £7.6bn. The results for different business sectors are shown below:

We believe that this type of cyber crime is heavily influenced by prevailing market conditions. However, in the current market climate of this study, three business sectors were assessed to be significantly impacted by espionage:

- **aerospace and defence** – £1.2bn per annum – which is due to the large proportion of revenue that companies in this sector derive from large tendering competitions⁶²;
- **financial services** – £2.0bn per annum – which is due to extremely high transaction volumes and recent share price fluctuations in this sector;
- **mining** – £1.6bn per annum – which is due to both the increasing market value of raw minerals and the high level of mergers in this sector at present⁶³.

CUSTOMER DATA LOSS

The costs to businesses of customer data loss arising from cyber attacks have been determined using information from the Department for Business, Innovation and Skills (BIS)⁶⁴ combined with additional information from the Ponemon Institute⁶⁵.

For this type of cyber crime, these references indicate that the business sector is less important than the overall size of the company. Therefore, our approach considered the following sizes of company⁶⁶:

- small companies, defined as having less than 50 employees;
- medium-sized companies, with between 250 and 500 employees;
- Large companies, with more than 500 employees.

The cost of customer data loss in each of these three categories was estimated as follows:

- We took the number of reported incidents of data loss and multiplied these by estimates of the average number of records lost in each incident and the handling cost per record. We took account of number of other factors, including estimates from BIS of business disruption costs, direct financial losses and average costs for reputational damage.
- We carried out a sensitivity analysis to determine what the effect would be of larger costs associated with reputational damage and direct financial losses, because we believe they are underestimated in some sources of data⁶⁷.

The overall impact from data loss is estimated to be between £0.96bn and £1.44bn per annum. The level of uncertainty in our results is principally driven by the variability in our estimate for costs associated with reputational damage.

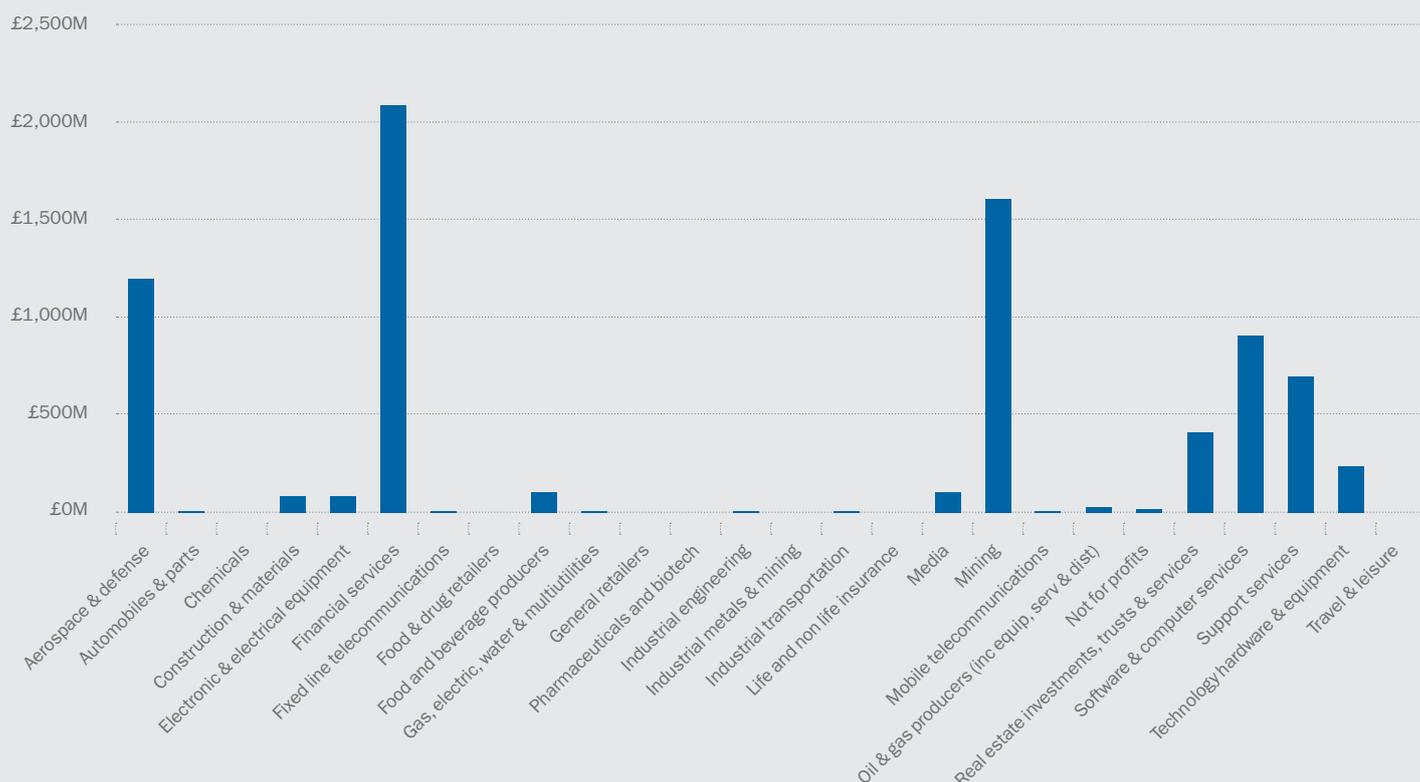
The results are shown below:

Business size	Best Case	Worst case
Small	£3.9m	£4.3m
Medium	£12m	£14m
Large	£940m	£1420m
Total	£0.96bn	£1.44bn

Annual costs to business of customer data loss through cyber crime

Estimates by UK business sector of the annual cost of industrial espionage by cyber criminals

Espionage impact by business sector



ONLINE THEFT FROM BUSINESS

As there are no reliable published estimates for direct online theft from business, our study attempted to estimate the likely impact by looking at the cash-flow per year across the different business sectors and making some assumptions about the level of cyber crime.

Our approach estimated a maximum percentage of annual cash-flow that a business sector could potentially tolerate being lost. This was multiplied by an estimate we made of the probability that businesses in this sector were subject to successful cyber attacks. Due to the sensitivity of the results to this estimate, we calculated three-point estimates of the worst case, best case and most likely costs.

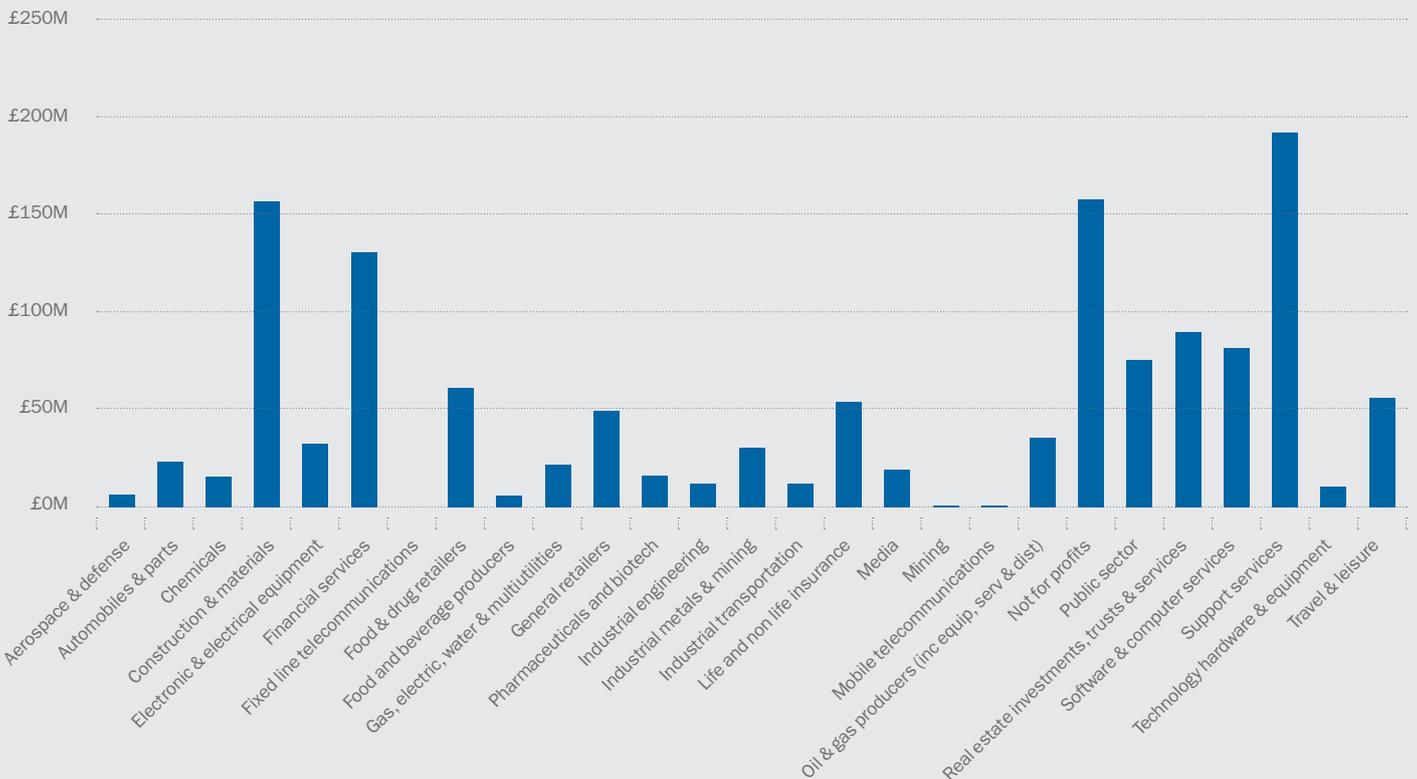
The figure below, shows the results across the business sectors for the most likely costs:

Overall, we estimate the most likely impact is £1.3bn per annum, with the best and worst case estimates £1.0bn and £2.7bn respectively. Our results show that **support services, the construction and materials industry** and the **not-for-profits sector** are most likely to be targeted.

We acknowledge that our approach to estimate the level of theft is based on a set of broad assumptions, but in the absence of data being available on actual levels of online theft, we consider them to be reasonable. In particular, the profile of online theft we have estimated for the business sector is driven by the amount of capital potentially at risk, and, one would therefore assume, the level of attractiveness the sector holds for cyber criminals.

Annual costs of online theft by cyber criminals by UK business sector

Online theft by business sector



Footnotes

- 62 For example, see the MOD Contracts Bulletin
- 63 PFK Deal Drivers
- 64 Department of Trade and Industry, 2004. Information Security Breaches Survey 2004 Technical Report
- 65 'Cost of UK data breaches 2010', Ponemon Institute, July 2010.
- 66 The definitions of company sizes are consistent with those used in the BERR 2008 Information Breach Survey.
- 67 Source: BIS

EXTORTION

This is one area in which we believe underreporting is prevalent⁶⁸. A successful extortion attempt is unlikely to be reported as this may cause further reputational damage with a low probability of recovering any of the money lost⁶⁹. We have therefore assumed that there are no reliable estimates of the true extent of cyber-extortion.

Our approach considered the combined turnover of business of small, medium and large size, and multiplied these by an estimate we made of the proportion of companies that would be vulnerable to extortion, the probability of an extortion attempt being made and the probability that it would be successful. The table below outlines the three point estimates we calculated using this approach.

Business size	Best case	Most likely	Worst case
Small	£12m	£20m	£24m
Medium	£13m	£27m	£34m
Large	£532m	£2,130m	£2,660m
Total	£0.56bn	£2.2bn	£2.7bn

Annual cost of extortion to UK businesses through cyber crime

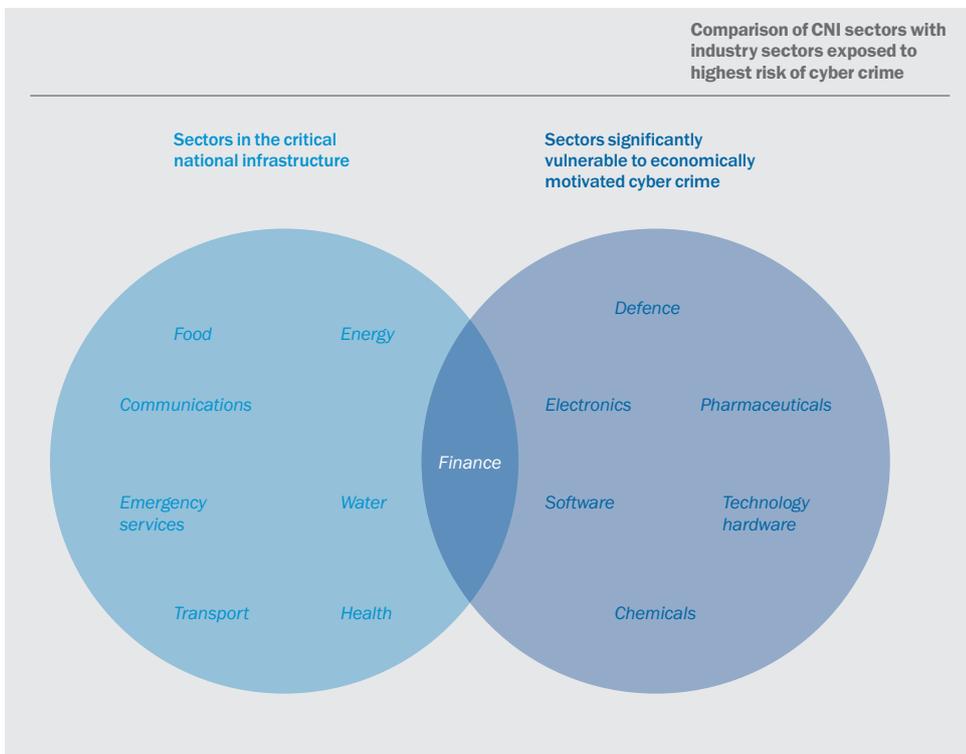
The overall impact on medium-sized business is lower because the number of companies that fall within this category is lower. The large variation in the three-point estimates is indicative of the uncertainty that remains in the true scale of extortion.

OTHER FINDINGS

This section presents an analysis of some of the key features of the results.

The impact of cyber crime extends far beyond the CNI

Our study has shown that the vast majority of business sectors assessed to be at greatest risk of cyber crime are not part of the Critical National Infrastructure (CNI)⁷⁰. Finance is the only sector that is both part of the CNI and assessed as being most at risk of cyber crime. This is illustrated below.



We believe that these results are because:

- companies within the CNI are established providers of core services that do not have a high level of IP;
- companies within the CNI tend to be stable, with limited M&A activity;
- companies within the CNI tend to provide services directly to the public, and very little of their turnover is generated through a commercial tendering process;
- companies within the CNI do not rely heavily on the use of the Internet to sell their products or services.

This is not to say that other types of cyber attacks are of no concern to the CNI. The CNI is a key target for cyber terrorism and cyber warfare, where the motive is to cause disruption and fear rather than to obtain financial revenue.

The Centre for the Protection of National Infrastructure (CPNI) currently provides advice and support to companies in the CNI on how they can improve their levels of protection against cyber attacks. We recognise that the CNI is exposed to other types of cyber risk, which are not instigated by financially-motivated criminals, but nevertheless recommend that at least the same emphasis should be given by the CPNI to the business sectors we have shown to be at the greatest risk of cyber crime.

Footnotes

- 68 For example, see Cyber-Extortion: 'The Elephant in the Server Room', Adam J. Sulkowski and Timothy Shea, May 2007
 69 Ibid
 70 For a definition of the CNI see the Centre for the Protection of the National Infrastructure web site, www.cpni.gov.uk

The costs of cyber crime vary considerably across business sectors

We found that there are large variations in the profile of cyber crime across different business sectors. We believe that this is due to a number of factors, which may include:

- **The sectors most affected are outside the CNI**, and so have not necessarily had the levels of regulation or investment in infrastructure or, resources to tackle cyber crime in the same way as those sectors that do fall under CPNI's principal remit. The only exception to this is the financial sector.
- **Each sector has a very different cyber risk profile**, and this can be due to several variables, such as the online presence of companies in the sector typically, the amount of liquidity they hold, the current market activity they engage in and the investment in IP and security they make.
- **The scale of IP theft across sectors differs depending on its value, because** companies in some sectors invest more heavily in IP than others, or consider IP generation more critical to their strategic growth.
- **The loss to business is much larger than the loss to citizens**, because, it seems, that cyber criminals can make more money from successful attacks on businesses through IP theft, online theft, espionage and customer data loss.
- **We believe that there are significant under-reporting issues in some cyber crime areas**, which may arise from lack of awareness or reputational considerations on the one hand, but also because of uncertainty of where to report, whether it will make a difference and confusion about when a cyber criminal attack is actually taking place on the other.
- **Some types of cyber crime may be much larger or smaller in scale than we estimate**, especially in areas which are typically undetected, under-reported or not investigated. For example, online extortion is very difficult to estimate as no information on its scale is publically available.
- **There are high knock-on indirect economic effects of cyber crime** which compound the estimates made in this study. Examples include the growth and increasing influence of highly organised criminal organisations and activity, and the potential re-investment of cyber criminal proceeds into other criminal activities, such as drug dealing and human trafficking.
- **Some economically-motivated cybercrimes on businesses and the Government can cause other harm to individual citizens, which magnifies the impact of the original crime**. For instance, businesses that are severely impacted by cyber crime may have to reduce staff levels accordingly to maintain their profit margins. This can lead to job losses and less consumer spending, which in turn, reduces the cash flow to organisations and creates a vicious circle.

The cost of cyber crime is significant and growing

Cyber crime costs the UK economy an estimated £27bn per annum. For the cyber criminals – who may be individuals, organised criminal groups or even nation states – it is highly lucrative and the barriers to entry are low. The ease of access to and relative anonymity provided by ICT lowers the risk of being caught while making crimes straightforward to conduct.

Additional work is needed to understand the cyber criminal's 'business model', however, which could draw upon knowledge being rapidly assimilated by law enforcement organisations and through research being conducted by 'think tanks' and academia. Through this model, more holistic approaches for countering cyber crime can be developed, seeking to exploit weaknesses in their end-to-end process, including striking at the dependencies that cyber criminals have on legitimate ICT infrastructure and service providers.

The impact of cyber crime is felt most by UK business

Although our study shows that cyber crime has a considerable impact on citizens and the Government, the main loser – at a total estimated cost of £21bn – is UK business, which suffers from high levels of intellectual property theft and espionage.

The impact of cyber crime does not fall equally across industry sectors. The most seriously affected businesses are from sectors not traditionally viewed as targets of cyber attacks. And, although the Government continues to focus on protecting the Critical National Infrastructure, providers of software and computer services, financial services, pharmaceutical and biotech and electronic and electrical equipment are at a particular risk from cyber crime. Without urgent measures to prevent the haemorrhaging of valuable intellectual property, the cost of cyber crime is likely to rise even further in the future as UK businesses increase their reliance on ICT.

The results of the current economic study suggest that businesses need to look again at their defences to determine whether their information is indeed well protected. Encouraging companies in all sectors to make investments in improved cyber security, based on improved risk assessments, is likely to considerably reduce the economic impact of cyber crime on the UK.

The UK needs to build a comprehensive picture of cyber crime

Although the existence of cyber crime in the UK economy appears endemic, efforts to tackle it seem to be more tactical than strategic. We believe that the potential for reputational damage is inhibiting the reporting of cyber crime. The problem is compounded by the lack of a clear reporting mechanism and the perception that, even if crimes were reported, little can be done. Additional efforts by the Government and businesses to measure and improve their understanding of the level of cyber crime would allow responses to be targeted more effectively.

Therefore, we recommend that selected companies from within the most affected business sectors are approached in confidence to help the Government build a more accurate assessment of IP theft and espionage. This would not only increase the awareness of the issues by individual companies, helping them to conduct detailed investigations into their losses from different types of cyber crime, but also contribute to a more accurate and comprehensive picture of cyber crime across the UK.

At the same time, we believe UK businesses should be provided with a Government-sponsored, authoritative, online and interactive service to promote more widespread awareness and the adoption of best practice in protection from cyber crime. Such a service could also provide a central reporting mechanism to allow businesses to report cyber crime, anonymously if necessary.

CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS

Footnote

70 "Business and the cyber threat: unknowingly under siege?", Detica security monitor, December 2010

ANNEX A: ORGANISATIONS CONSULTED

Representatives from the following government departments were consulted during the study:

- Serious Organised Crime Agency (SOCA)
- Intellectual Property Office (IPO)
- Police Central E-crime Unit (PCeU)
- Centre for the Protection of the National Infrastructure (CPNI)
- The Department for Business Innovation and Skills (BIS)

In addition, several discussions were held with senior security staff within some of the most high profile organisations across industry sectors. For the purposes of this report, these businesses have remained anonymous.

ANNEX B: BUSINESS SECTOR BACKGROUND

This appendix provides background information on the key business sectors that are potentially at greatest threat from cyber crime. The information was used to inform the development of the cyber crime impact model.

It must be noted that, whilst every effort was made in this study to obtain the most authoritative, reliable and up to date information on each industry sector, this data has not always been available. Although changing market conditions and new research may, therefore, alter the assessments below, we hope that the framework provided in this study will help in future studies and evaluations of the total cost of cyber crime to the UK.

Aerospace and defence

The UK aerospace industry is the world's largest outside the USA with a 17 per cent share of the global market. It has an annual turnover of around £139bn per annum according to the UK National Accounts Blue Book 2010. It directly employs 101,000 workers, and supports a total of 230,000 jobs across the UK economy. It also contains a highly skilled workforce, with 36 per cent of all employees having a university degree or equivalent. The UK defence industry provides high-value employment, technology, innovation and exports and is a core element of the UK manufacturing industry.

The UK aerospace and defence sectors continue to represent significant long-term growth opportunities for the UK economy, with international companies attracted by the UK's open market, competitive supply base and strong government support for R&D. The aerospace and defence sectors spent around £2bn on R&D in total and were the second largest contributor to R&D in the UK1000 and the seventh largest in the G1000 in 2008. In 2008, the three giants of the UK aerospace sector – Airbus, BAE Systems and Rolls-Royce – collectively spent almost £1.2bn on R&D.

Due to the high levels of revenue generated by this market, combined with fierce international competitiveness and substantial investment in R&D, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations), IP theft and share price manipulation (through state sponsored activity).

Automobiles and parts

The turnover of the UK automotive sector is £24bn, contributing approximately 1.5 per cent of GDP and generating some £10.2bn value added. The industry employs some 715,000 people, both directly in vehicle manufacturing and in the supply and distribution chain. About half of added value comes from manufacturing and assembly, which represents about 15 per cent of total UK manufacturing value added. The UK sector's particular strengths include design engineering, especially advanced technology in motorsport. It is also increasingly becoming a centre for engine production and in 'premium' cars.

The automobiles and parts sector was the fifth largest contributor to R&D in the UK1000 and the second largest in the G1000 in 2008. Overall the industry is currently investing over £1bn annually in new plant and technology, equivalent to 13 per cent of gross value-added. The UK is also a centre for design engineering where around 7,500 people are employed, generating a turnover of some £650m, with around 65 per cent exported. Automotive R&D accounted for six per cent of total UK R&D and the innovation generated can support other United Kingdom industries.

Due to the high levels of revenue generated by this market, combined with fierce international competitiveness and substantial investment in R&D, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations), IP theft and share price manipulation (through state sponsored activity).

ANNEXES

Chemicals

The chemical industry is one of the largest manufacturing industries in the UK, with a turnover of £55bn and predicted continued good growth despite the economic downturn. With an 8.2 per cent share of the world market, the UK chemical industry provides direct employment for 214,000 people and supports several hundred thousand additional jobs throughout the economy. The industry spends in excess of £2 billion per year on new capital investment.

The chemical industry is very efficient, delivering a value added per employee of nearly twice that of the UK manufacturing average. Today, the UK chemical industry focuses 60 per cent of its production on the specialist sector. The result is an innovative industry, strongly assisted by major research and development centres and funding initiatives which are enabling UK-based businesses to capitalise on new materials and products to secure competitive advantage.

The R&D expenditure by the UK chemicals industry is £3.8bn per annum, and amounts to more than 10 per cent of industry sales. Furthermore, the UK government offers tax credits to UK-based business engaged in R&D. As a result, the UK has developed dynamic, innovative clusters in a wide range of technologies and many overseas companies have established R&D centres in the UK to capitalise on this open innovation 'ecosystem'. Around 45 per cent of all business R&D undertaken in the UK is funded by overseas-owned companies.

Due to the high levels of revenue generated by this market, combined with fierce international competitiveness and substantial investment in R&D, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations) and IP theft (through state sponsored activity).

Electronic and electrical equipment services

The UK electronics industry is worth £55bn a year and is the fifth largest in the world. It employs over 250,000 people in the UK in more than 11,000 workplaces and represents ten per cent of the UK manufacturing industry. Electronics is pervasive and underpins virtually every other sector of economic activity. It is a key enabling technology in every other sector providing labour saving devices, driving the development of high-speed communications and information processing, and transforming entertainment and business. Of the UK EPES manufacturing businesses, more than 98 per cent are below the 250 employee threshold that defines them as small or medium sized enterprises, and around two thirds are 'Micro' enterprises with less than 10 employees. These small or medium sized enterprises account for around half the work force and turnover.

The R&D expenditure by the electronics sector is £5.7bn per annum and accounts for 7.2 per cent of the UK R&D investment total. The UK hosts nearly a third of Europe's silicon design companies.

Due to the high levels of revenue generated by this market, combined with significant investment in R&D and the high levels of medium and smaller companies, this sector is likely to be affected by cyber crime through industrial espionage, share price manipulation (through international corporations), IP theft (through state sponsored activity) and service denial (as there is a high level of online reliance by smaller companies).

Financial services

The UK Financial Services industry (including banks) has an annual turnover of around £812bn according to the 2010 Blue Book. It directly employed just over one million people in 2009 and despite the recent financial crisis, its net exports grew to £50bn in 2008. Over the last year, the UK financial services sector remained the largest in Europe, while London retained its mantle as the world's international centre of choice for more financial institutions and investors than any other city globally. The impact of financial services, however, goes well beyond the sector's direct contribution to the UK economy. Since finance underpins everything in an economy and society, its availability and stability are necessary to support societal needs. The industry provides a critical underpinning for the generation, accumulation and transfer of wealth and provides essential capital for business growth. Innovations in financial services also help governments, businesses and individuals to invest and take risks in a measured, more considered manner.

The banking sector was the fourth largest contributor to R&D in the UK1000 and fifteenth in the G1000 in 2008. Three banks were among the top 25 UK investors in the UK1000: RBS, HSBC and Barclays continue to dominate R&D investment in the UK banking sector. Together they accounted for 88 per cent of the sector total and over five per cent of the UK1000 spend in 2008. According to the BIS 2009 R&D scorecard, the financial sector (including banks) invested around £1.8bn in R&D activity.

Due to the high levels of revenue generated by this market, combined with substantial investment in R&D and a high online presence and reliance on technology, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations) share price manipulation (through state sponsored activity), online theft and online fraud (as there is a high level of concentrated financial liquidity).

Food and beverages

The UK Food and Beverage manufacturing industry is the single largest manufacturing sector in the UK, with a turnover of £72.8bn and a gross value added of £21.6bn, accounting for 15 per cent of the total manufacturing sector. Employing more than 500,000 people, it makes a huge contribution to the economy and positions the UK as the fifth largest exporter of value-added food and drink. All this economic activity is carried out by just over 7,000 food and drink enterprises – many of which are small companies employing less than 10 people.

The food and beverage sector accounts for over four per cent of the total R&D spend reported in the UK. Due to the highly competitive nature of the industry, there are over 1,500 new products introduced each quarter. The mix of product and process innovation is a core strength of the sector. Due to its size, direct links to health outcomes and its impact on emissions from production and logistics, the food and drink sector should have a strategic focus in the UK.

Due to the high levels of revenue generated by this market, this sector is likely to be affected by cyber crime through online theft and online fraud (as there is a high level of concentrated financial liquidity).

Healthcare, pharmaceutical and biotech

The pharmaceuticals and biotechnology industries contributed around 4 per cent of total UK value added in 2008, while the healthcare equipment and services sector contributed 0.5 per cent. The total annual turnover for all UK healthcare, pharmaceuticals and biotech industries was around £29bn.

The UK-based healthcare technology industry plays a significant role in contributing to patient care, public healthcare and the national economy with values of £5.6bn annual sales in 2007 and £5.4bn in exports in 2008.

The UK is one of the world's largest exporters of pharmaceuticals by value. Industry exports in 2005 were £12.2bn and created a trade surplus of £3.4bn. UK domestic market accounts for four per cent of world consumption.

The UK's medical biotechnology sector is the most mature in Europe and contains approximately 450 biotechnology businesses in the UK employing 21,830 with revenues around £2.63bn

The pharmaceutical industry invests around 30 per cent of its sales in research. This amounts to nearly £4bn, or more than £10m a day. The pharmaceuticals and biotechnology sector was the largest contributor to R&D in both the UK1000 and the G1000 in 2008.

Due to the high levels of revenue generated by this market, combined with high investment in R&D and the high levels of medium and smaller companies, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations) IP theft (through state sponsored activity), and service denial (as there is a high level of online reliance by smaller companies).

Industrial engineering

In 2007 the UK's total exports in the engineering sector exceeded £109bn, with manufacturing accounting for 14 per cent of the UK's GDP and 55 per cent of its exports. There are some 2.9m people employed in UK manufacturing. Examples of industrial engineering include nanotechnology, ceramics, plastics processing, printing and publishing, processing and packaging equipment, automation, and solids and materials handling

The UK is the world's sixth-largest engineering and manufacturing base and engineering and manufacturing industries spent £10.8bn on R&D in 2006.

Due to the high levels of revenue generated by this market, combined with high investment in R&D and the high levels of medium and smaller companies, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations) IP theft (through state sponsored activity), and service denial (as there is a high level of online reliance by smaller companies).

Mobile telecommunications

The contribution of the mobile telephone industry to UK GDP was £40.6bn in 2009. This was 2.2 per cent of the UK's total economic output and the industry contributes £15bn a year to government finances. The sector is responsible for nearly 200,000 jobs. The UK (mobile) market is considered to be one of the most competitive in the world with well established 2G GSM (Global Systems for Mobile Communications) and 3G UMTS (Universal Mobile Telecommunications Systems) operators. Since the privatisation of the incumbent operator BT in 1984, competition has developed strongly. There are now approximately 170 fixed telecommunications providers, five mobile providers, 59 mobile service providers and 700 Internet service providers.

The mobile telecommunications sectors were the sixteenth largest contributor to R&D in the UK1000 in 2008. Both BT and Vodafone dominated R&D spending in the UK telecommunications sectors, as together they spent 93 per cent of the sector total, and five per cent of the overall UK1000 spend. R&D decreased in the UK telecommunications sectors in 2008, while sales grew. Of the biggest investors, only Vodafone grew its R&D investment (by 20 per cent) more quickly than its sales.

Due to the high levels of revenue generated by this market, combined with significant investment in R&D and the high levels of customer data, this sector is likely to be affected by cyber crime through industrial espionage (through international corporations) IP theft (through state sponsored activity), and online theft, customer data theft and online fraud (as there is a high level of customers, transactions and profits).

Not-for profits

The UK Not for Profits sector generates a total of £11.1bn revenue and comprises of both charities (with £52bn generated and 188,000 organizations) and higher educational institutions (with £59bn generated). Some charities are large in both income and staffing, but more than half of registered charities have an annual income of less than £10,000. For higher educational institutions, there is a substantial employment effect with around 670,000 jobs being created throughout the economy in 2007/08. Of these some 372,000 people were directly employed by universities and colleges. There is further evidence of the importance of international students to the sector and the wider economy. One significant impact is the volume of personal off-campus expenditure of these students, which amounted to £2.3bn in 2008.

Charitable funding of UK R&D has been rising in real terms since 2004 and reached around £950m in 2008-09. Most research charities do not consider the funding of university infrastructure their responsibility, although many contribute to it. Higher education institutions income is around £3.7bn through research grants and contracts, through around 2,000 UK public sources and around 1,000 private sources.

Due to the high levels of revenue generated by this market, combined with substantial investment in R&D, this sector is likely to be affected by cyber crime through IP theft (through state sponsored activities), customer data theft (through large databases containing personal information in charities) and industrial espionage (through international corporations).

Oil and gas

The oil and gas industry is one of the largest UK economic contributors in terms of added value (measured as the value of sales minus production costs), accounting for £22bn in 2006. This amounted to 13 per cent of the production and manufacturing industry total in the UK. In 2007, the upstream oil and gas industry invested £4.9bn in capital and £1.3bn in exploration and spent £6.2bn in operations, making a total expenditure for the year of £12.4bn. The industry now provides employment for 450,000 people and delivers around £21bn in taxes every year, both from direct taxation of production and the wider economic activities of the UK supply chain. In 2009, the UK's balance of trade in goods and services was boosted by oil and gas production by up to £27bn.

In 2009, the sector was the largest industrial investor, spending £5.7bn on R&D activities. Shell was the largest investor in research and development among the major oil firms spending nearly £800m on the research and development of technologies to produce more energy, and more efficient fuels and products.

Due to the high levels of revenue generated by this market, combined with significant investment in R&D and the high dependency level of other sectors on the energy produced by oil and gas, this sector is likely to be affected by cyber crime through industrial espionage, share price manipulation (through international corporations) and IP theft (through state sponsored activity).

Software and computer services

The UK is one of the largest ICT markets in Europe, worth almost £120bn in 2009 and employing over one million people. The software and computer services industry is central to the UK economy and a key source of competitiveness for all sectors, opening up new markets, increasing performance and driving productivity. The UK's IT industry produces an annual GVA of £30.6bn, three per cent of the total UK economy. Continued IT adoption and exploitation has the capacity to generate an additional £35bn of GVA to the UK economy over the next five to seven years. In the UK 1.2m people are employed in the IT workforce (597,000 in the IT industry itself and 650,000 IT professionals working in other industries). These are the people upon which the 22m employees who use IT in their daily work rely upon for the creation, implementation and operation of systems, services and communications, forming the backbone of companies across the UK. There are 154 software and computer services companies in the UK1000, more than in any other sector

In 2008, the software and computer services sector was the third largest contributor to R&D in both the UK1000 and the G1000. R&D spending by companies in the UK software and computer services sector remained more fragmented than in other sectors: the six largest companies in terms of R&D spent 47 per cent of the sector total.

Due to the high levels of revenue generated by this market, combined with significant investment in R&D and the high online presence and dependency level of other sectors on the capabilities produced by software and computers, this sector is likely to be affected by cyber crime through industrial espionage, share price manipulation (through international corporations), IP theft (through state sponsored activity) and extortion and online fraud (by cyber criminal organizations).

Technology and hardware services

The UK technology and hardware services generate £86bn a year and are growing in significance. The sector also makes a positive contribution to UK trade, with export in services in particular bringing in an estimated £1.4bn for April-June 2009 alone. The UK's technology sector will continue to grow in size and importance over the next decade. Next generation technologies are using semantic approaches to catalogue information and compile more accurate and personalised responses to information queries, essential given the increasing volume of data on the internet.

The R&D expenditure by the electronics sector is around £1bn per annum and has included initiatives such as the £30m Centre for Secure Information Technologies at Queen's University, Belfast, which will become the UK's principal centre for the development of technology to counter malicious cyber attacks.

Due to the high levels of revenue generated by this market, combined with significant investment in R&D and the high levels of medium and smaller companies, this sector is likely to be affected by cyber crime through industrial espionage, share price manipulation (through international corporations), IP theft (through state sponsored activity) and service denial (as there is a high level of online reliance by smaller companies).

About Detica

Detica delivers information intelligence solutions to government and commercial customers. We help them collect, exploit and manage data so they can deliver critical business services more effectively and economically. We also develop solutions to strengthen national security and resilience.

We integrate and deliver world-class solutions to our customers' most complex operational problems – often applying our own unique intellectual property. Our services include cyber security, managing risk and compliance, data analytics, systems integration and managed services, strategy and business change and the development of innovative software and hardware technologies.

Detica is part of BAE Systems, a global defence and security company with over 100,000 employees worldwide. BAE Systems delivers a full range of products and services for air, land and naval forces, as well as advanced electronics, security, information technology solutions and customer support services.

For more information contact:

Detica Limited
Surrey Research Park
Guildford
Surrey, GU2 7YP
United Kingdom
+44 (0) 1483 816000

E: info@detica.com
www.detica.com

© 2011 Detica Limited. ALL RIGHTS RESERVED. Detica, the Detica logo and/or names of Detica products referenced herein are trademarks of Detica Limited and/or its affiliated companies and may be registered in certain jurisdictions. Detica Limited is registered in England (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7YP

02.11.DET.CCR.001