THE COST OF CYBER CRIME.

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

CabinetOffice

Detica

EXECUTIVE SUMMARY

WHY MEASURE 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[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 2009[3]. 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.

As well as significant benefits, the technology has also enabled old crimes to be committed in new and more subtle ways. In its National Security Strategy[4], 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 not been able to provide a justifiable estimate of economic impact and have failed to address the breadth of the problem. Therefore, the Office of Cyber Security and Information Assurance (OCSIA) worked 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 will thus benefit from this 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. Cyber criminals can range from foreign intelligence services and large organised crime groups, to disreputable (but otherwise legitimate) companies and individuals or small groups of opportunists.

In our study, we have focused on less-understood cyber crimes, including:

- identity theft and online scams affecting UK citizens;
- IP theft, industrial 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. In our study we have not included crimes that lack an overriding financial motive. Nor have we investigated either the attack methods used by cyber criminals or the origins of such attacks.

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 IP theft and industrial espionage.

CRIME'S GONE DIGITAL. NEW TECHNOLOGY HAS ENABLED OLD CRIMES TO BE COMMITTED IN NEW AND MORE SUBTLE WAYS.

Footnotes

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 "A strong Britain in an age of uncertainty", National Security Strategy, October 2010

STUDY METHODOLOGY

To address the complexity of less understood cyber crime we have 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 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 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.

During this study, 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.

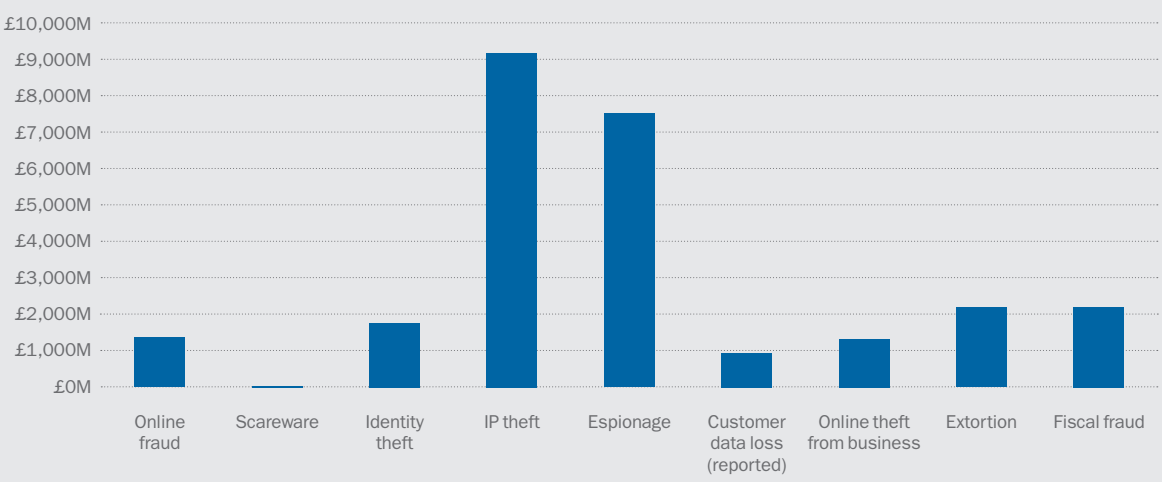
CONCLUSIONS AND RECOMMENDATIONS

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 is not felt equally. Our results 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. 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.

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.

Cost of different types of cyber crime to the UK economy



COST TO CITIZENS

Our estimate for the economic cost of cyber crime to UK citizens is **£3.1bn** per annum. This estimate includes:

- **£1.7bn per annum for identity theft** (similar estimates by CIFAS[5] and the IFSC[6] were £1.7bn and £1.2bn per annum respectively);
- **£1.4bn per annum for online scams;**
- **£30m for scareware and fake anti-virus software** (based on data published by Symantec[7]).

Citizens can help themselves to 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. No defences are foolproof, though, and even well-prepared citizens may suffer a range of costs as a consequence of and in responding to cyber crime.

The prevalence of these types of cyber crimes means that their aggregate effect is detrimental to the UK economy. Furthermore, indirect macro-economic effects could also occur, for example, from a general loss of confidence in services such as online banking.

COST TO THE GOVERNMENT

Our estimate for the economic cost of cyber crime to the Government is **£2.2bn** per annum.

We took information from the National Fraud Authority Annual Fraud Indicator[8], which estimates the total cost of tax and benefits fraud, local government and central government fraud, NHS fraud and pension fraud. The total cost was combined with an estimate from the NFA 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 attacks due in the main to the volume of transactions now conducted online. 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.

The Government and public sector bodies spend significant sums of money on security to reduce the impact of all types of crime in the UK. The formation of the Police Central e-Crime Unit, for example, demonstrates a wider commitment from the Government to tackling cyber crime in particular. We have not included these costs in our study, though, because these resources also provide benefits in combating many other types of crime and insecurity.

Finally, there are significant knock-on effects for the Government, particularly because increasing levels of fiscal fraud committed by cyber criminals 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.

COST TO BUSINESSES

Our estimate for the economic cost of cyber crime to UK businesses is **£21bn** per annum. This estimate includes:

- **£9.2bn per annum from IP theft**, which has the greatest economic impact of any type of cyber crime considered in this study, and is likely to have the largest impact on companies that create significant quantities of IP or those whose IP is relatively easy to exploit;
- **£7.6bn per annum from industrial espionage** (involving the theft and exploitation of non-IP-related data), which affects companies involved in open-tendering competitions, that rely on large numbers of financial transactions or that are affected (or can be affected) by large share price movements;
- **£2.2bn per annum from extortion**, with large companies being targeted (although our estimates are largely illustrative because we believe this type of cyber crime goes largely unreported);
- **£1.3bn per annum from direct online theft**, with cyber criminals targeting support services, financial services, the construction and materials industry, and the not-for-profit sector.
- **£1bn per annum from the loss or theft of customer data**, with the significant majority of the impact falling on large companies with more than 500 employees.

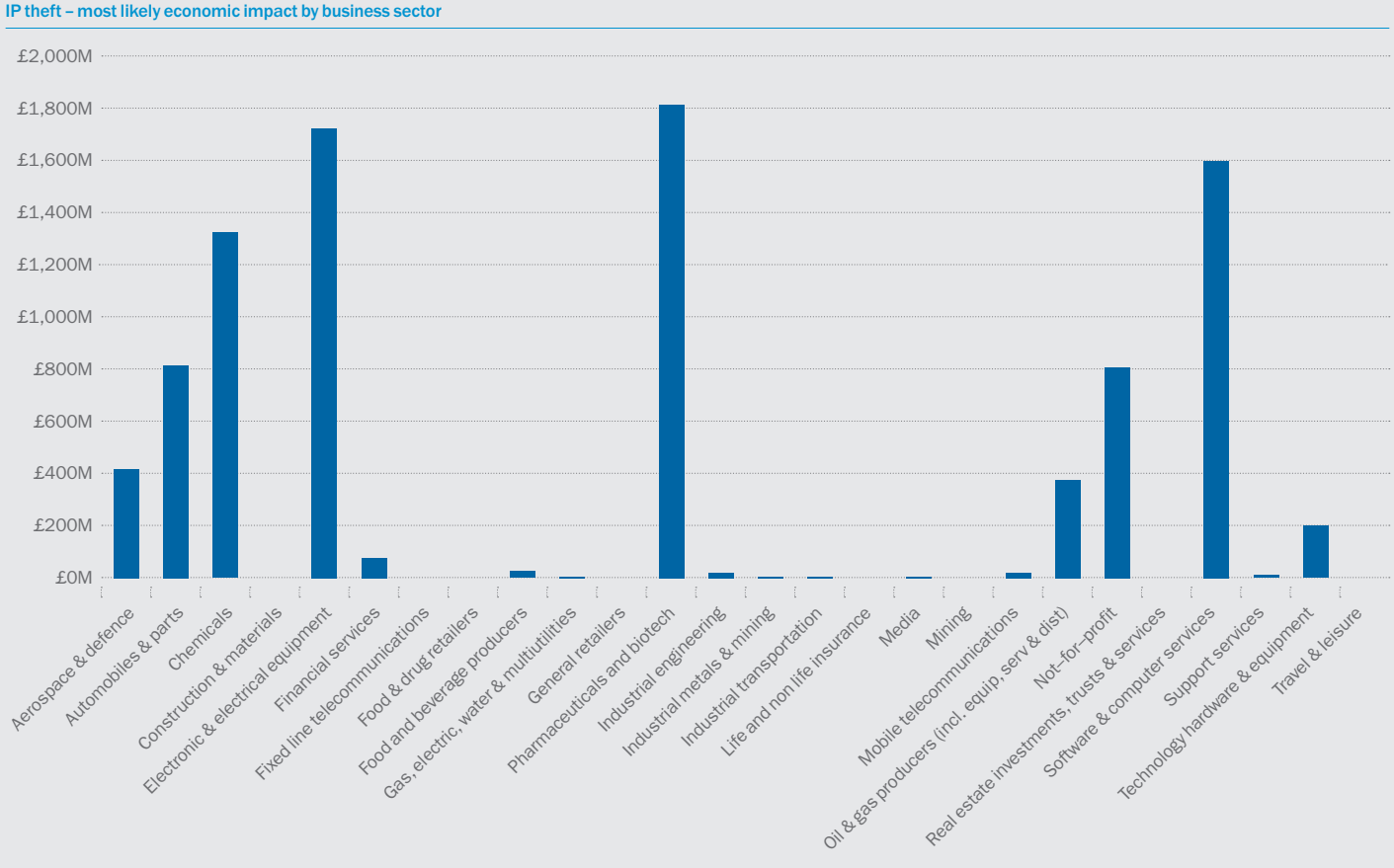
In anticipation of coming under attack by cyber criminals, many UK businesses are investing in stronger physical security, such as segregated networks, advanced intruder detection hardware, or training initiatives to increase their employees' awareness of cyber crime. These initiatives are particularly important for IP-rich business sectors, such as the pharmaceutical and biotechnology sectors, which invest heavily in research and development and rely on it to create market advantage in a fiercely competitive global industry.

IP THEFT

With the exception of the well-understood and documented copyright theft issue, 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. But calculating the impact of this type of less-publicised IP theft is complex. Our approach produced three-point estimates for the economic value of IP by taking published figures for the value added to the economy per year in each sector and estimating the fraction attributable to IP.

Our results show that several business sectors are likely to be affected by IP theft because they either generate large volumes of IP or their IP can be exploited with relative ease. However, although no business sector is likely to be entirely immune from IP theft, the impact of cyber attacks is likely to be much smaller in sectors where relatively low volumes of IP are created.

Cost of IP theft by industry sector



Footnotes

5 CIFAS, 2006. Identity Fraud – What About The Victim?
6 'New Estimate of Cost of Identity Fraud to the UK Economy', Identity Fraud Steering Group (IFSC), 2008
7 Symantec, 2009. Report on Rogue Security Software
8 National Fraud Authority, 2010. Annual Fraud Indicator

COST TO BUSINESSES (CONTINUED)

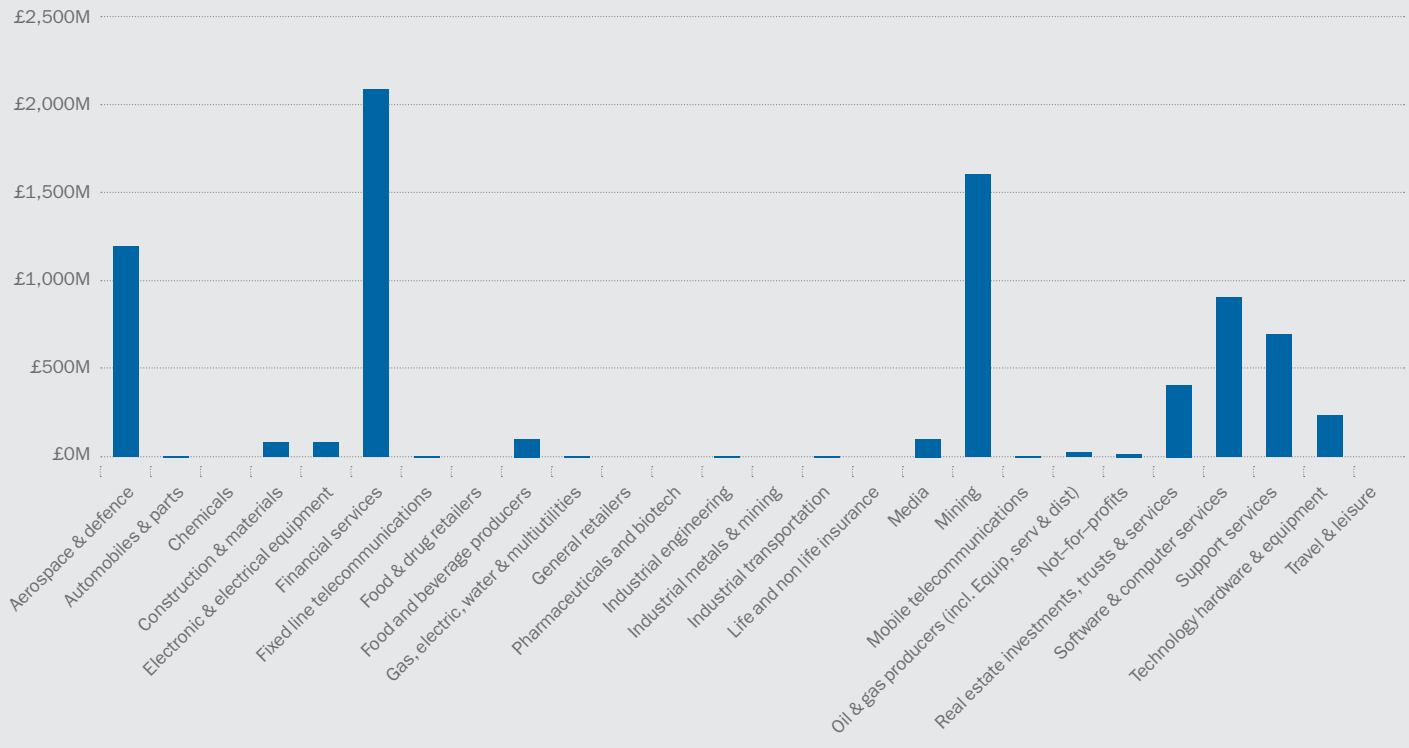
INDUSTRIAL ESPIONAGE

Our study investigated the loss of competition-sensitive information, which could impact a company's chances of winning open tenders, and the loss of information relating to mergers and acquisitions (M&A), which could enable cyber criminals to gain advantage from share price movements.

We believe that the impact of this type of cyber crime is heavily influenced by prevailing market conditions. However, in our 'snapshot' for 2010, the most affected business sectors are those where the proportion of revenue that companies derive from tendering competitions is high, where there are high transaction volumes, high costs of raw materials, large share price fluctuations, or high levels of M&A activity.

Cost of industrial espionage by industry sector

Espionage impact by business sector



CONCLUSIONS AND RECOMMENDATIONS

THE COST OF CYBER CRIME IS SIGNIFICANT AND GROWING

Cyber crime is a national scale issue, which costs the UK economy an estimated **£27bn** per annum. For the cyber criminals – who may be individuals, organised crime 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 BUSINESSES

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 IP theft and espionage. But 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, companies in IP-rich industries are at a particular risk from cyber crime. The results of this study suggest that businesses of all sectors 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, the cost of cyber crime is likely to rise even further in the future as industry increases its reliance on ICT. 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.

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

02.11.DET.CCRSUMMARY.001