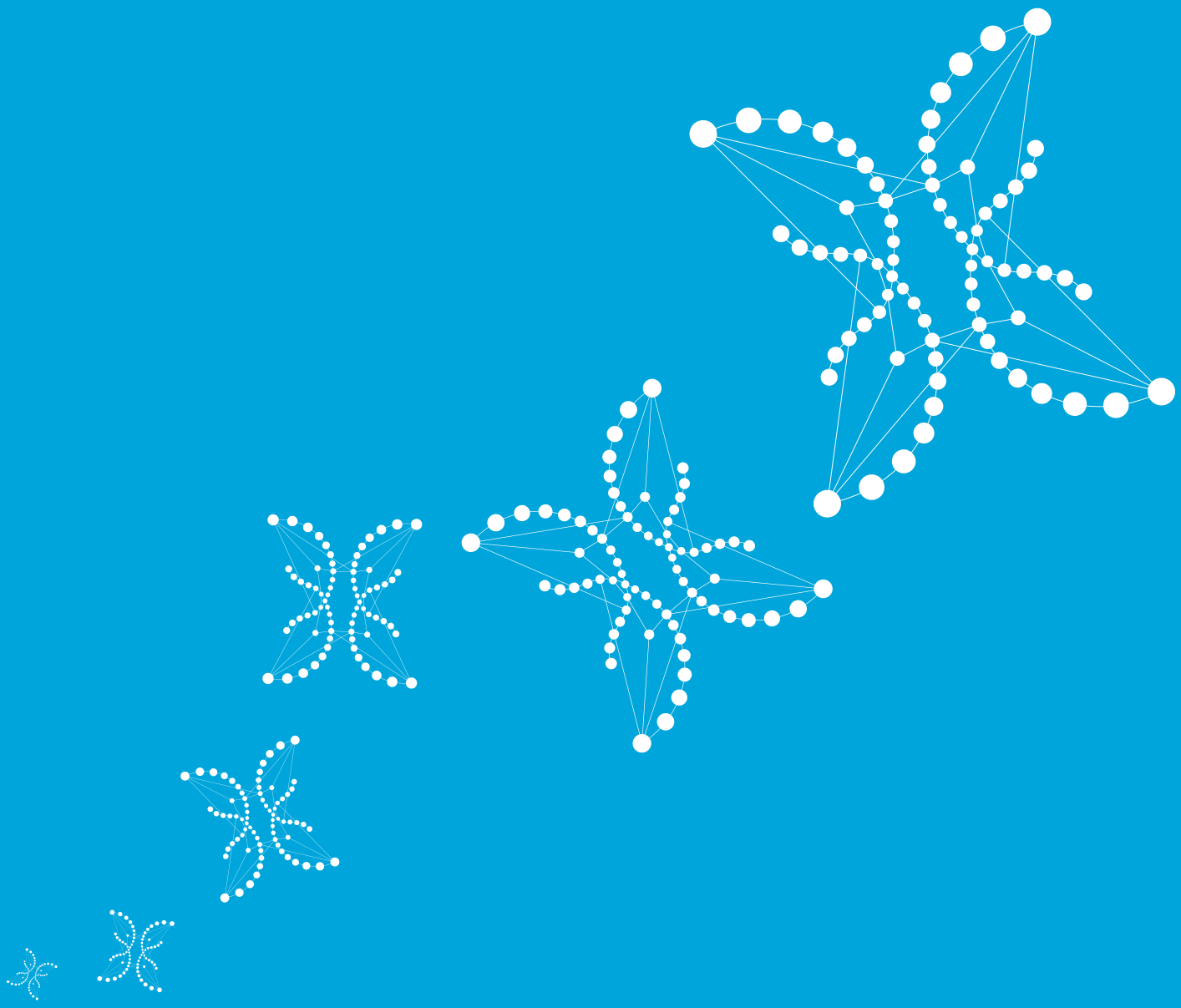
Research report: July 2009

NESTA Making Innovation Flourish

Crime online

Cybercrime and illegal innovation

Howard Rush, Chris Smith, Erika Kraemer-Mbula
and Puay Tang, CENTRIM, University of Brighton



Executive Summary

With the growing sophistication and use of information technology, the past decade has seen a major growth in cybercrime. Broadly described, cybercrime refers to all types of crime that exploit modern telecommunications networks, in which computers or computer networks are used for criminal activity.

This report focuses exclusively on financial cybercrime, specifically credit card fraud and identity theft. Of course, there are other forms of cybercrime ranging from paedophile networks to denial of service operations that are beyond the scope of this study.

Financial cybercrime has increased dramatically in recent years and looks set to increase further as the proliferation of communications technology proceeds apace and reaches regions of the world with many underemployed poor people with information technology skills who can take advantage of cybercrime opportunities. The current global recession will likely increase this trend still further.

Information and Data

The reporting of cybercrime and related issues has grown significantly in recent months. Without exception, every week sees media reports of large-scale cybercrime activities. Recent reports have included:

- A million people may be phishing scam victims (Telegraph.co.uk, 7th March 2009)
- Spam rises 150 per cent in two months (Australian IT, 8th March 2009)
- Worm infects millions of computers worldwide (The New York Times, 28th January 2009)
- Cyber scams on the up in the downturn (The Australian Business with the Wall Street Journal, 30th January 2009)
- Cybercrime wave sweeping Britain (BBC News, 30th October 2008)
- Businesses risk $1 trillion losses from data theft (The Washington Post, 30th January 2009)
- Russia and China accused of harbouring cybercriminals (Times Online, 12th October 2008)

Behind these sensational headlines, however, the data that fuels the current debate on the contemporary dynamics of cybercrime are far from straightforward. No reliable

'official' statistics exist yet. Although many associations and groups regularly publish their own estimates, they are impossible to compare. Moreover, the reliability of these figures is regularly criticised as being over or under estimating the true picture, depending upon the vested interests of the organisation responsible.

Trends in Credit Card Fraud

Credit card details can be obtained illegally by card skimming, phishing or by accessing personal computers and database systems using Trojans or by hacking.[1] As credit and debit cards continue to replace cash and cheques and as online Internet sales increase, the opportunities for cybercrime activity are also growing. Credit card theft has increased at an average rate of 10 per cent a year. In the UK alone, credit card fraud was estimated to have reached over £500 million in 2007. The introduction of 'chip and pin' technology – where consumers must use a pin code rather than a signature to verify their identity when using a card – slowed the growth of credit card fraud in 2005 and 2006 but its effectiveness may not last much longer as criminals find ways to circumvent these security measures.

Identity Theft

The misappropriation of identity details and their subsequent use for criminal activity are both changing and increasing. Whereas once this was the domain of 'bin raiders' – criminals stealing from household bins – and mail thieves, identity theft now takes place online. Increasingly, cybercriminals are finding ways of taking over bank accounts – between 2007 and 2008 'take-over' fraud increased by 159 per cent. Though the technology for detection and prevention has also moved forward, continuous data breaches, primarily as a result of human error, are exposing personal information on a large scale. The proliferation of social networking websites is also providing cybercriminals with new areas to exploit as well as new areas for recruitment.

The Global Distribution of Cybercrime

As more and more regions of the world go online, cybercrime is finding new and more permissive environments. Especially in developing nations, cybercrime is gaining a foothold. Law enforcement agencies are struggling to respond, especially in places where legislative frameworks are weak or non-existent. The growth of cybercrime in Russia, India, China and Brazil is of particular concern.

[1] Definitions of each of these activities appear in the Appendix.

The Cybercrime Digital Ecosystem

This study has shown that management study's methodology is a useful tool for explaining, analysing and understanding cybercrime.

Value Chain Analysis

The concept of a value chain is a simple but very effective way to explain how innovation can help to tackle cybercrime. Value chains describe the sequence of activities that are required to make a product or service, from conception to delivery and disposal. They operate within an 'ecosystem' or environment where businesses cooperate and compete. This sequence of activities involves the combination of inputs from various actors, which are increasingly distributed globally. This idea emphasises the global reach of economic activities, and its central concern is to unpack the relationships between the actors involved in producing a good or service.

Value chain analysis allows us to grasp the big picture of cybercrime and give perspective to the individual anecdotes and isolated figures that are reported daily. It also highlights the need to understand the distribution of power along the chain. The cybercrime value chain is virtually coordinated by both buyers and producers of crimeware (malicious software designed to automate financial crime).

This analysis recognises the importance of the power asymmetries in global value chains, particularly who leads the overall character of the chain and who governs it? The concept of governance is crucial for three main reasons. First, leading actors in the chains can have a major impact in creating and shaping new markets. Second, leading actors will have a major role in determining the price, quality and speed of production. Third, leading actors will have a major role in determining the distribution of gains and profits along the chain.

Innovation is a major force for the continuous improvement of products and processes. However, value chain analysis stresses that innovation needs to be placed in a relative context, in particular, compared to competitors. 'Upgrading' is the term used for this process of innovation in an industry formed by many global actors competing and integrating with each other.

Dynamic Capabilities

The second component relates to capabilities. A firm's capability is "a collection of routines that confers upon an organisation's management the ability to produce significant outputs of a particular type". However, analysts argue that dynamic capabilities – the capacity to adapt to rapidly changing environments – are required to create and sustain competitive advantage in a changing business environment. Such capabilities therefore underpin the ability of an organisation to make best use of new equipment or technologies to produce novel and innovative products or services. They improve their productivity and competitive advantage. As with firms that deploy home-grown capabilities to create competitive advantage or a market niche, cybercriminals appear to also have some in-house capabilities to carry out their activities and easy access to buy in the required capabilities. In part, this may be due to a complete absence of norms and legislation and the eclectic mix of actors and their characteristics that exist within the cybercrime world.

Business Models

The third component of the cybercriminals' world is that of business models. The position of firms and its activities in the value chain is an important determinant of how it approaches business and generates a profit. Common to all definitions of business models is an emphasis upon how a firm makes money. Business models have the added attraction of being potentially comparable across industries. Therefore, in the context of this study, business models refer to the way in which different cybercriminals specifically generate revenue, and the nature of the arrangement they have with their customers and suppliers in the value chain.

Future Trends in Cybercrime

The organisational and technological capabilities of cybercriminals, especially in the absence of a global counter-strategy, will likely deepen and widen into the foreseeable future. As cyberspace develops further, so new opportunities will open up for organised crime groups.

Crimes such as electronic theft and fraud will occur more rapidly, reducing the likelihood of being caught in the act. Information about how to compromise a system will be available more quickly and to more people, which means that opportunistic criminals linked into networks of organised criminals will come to dominate and define the world of

cybercrime. The ability of criminals to use new technology will also have a major impact on the sort of crime we see. In cyberspace, we can expect this to be further magnified. The relationship between the offender and victim, in particular, may change, as neither is aware of the other's humanity which could see on-line offenders committing more extreme crimes. Equally, if victims have no contact with the offender, their attitudes to punishment may change, either through reduced demands for punishment, or an increase in those for harsher penalties.

Conclusions and Reponses

As the current recession deepens, cybercrime looks set to make an even greater impact.

In the UK **a national initiative is urgently required to tackle cybercrime**. It needs to be applied across the UK regions and nations, and it needs to be part of a genuinely transnational effort. European Union member states need to make common cause.

Given that so many cybercrime operations take place in developing countries, **aid agencies need to be persuaded to build on their police reform work to help address cybercrime.**

We as individuals need to learn how to make our personal IT systems more secure. Banks should help to incentivise such greater personal security, recognising that they have a vested interest in doing so as well as compensating their customers who become victims.

The private sector responses should be reviewed and analysed in search of best practice. **New legislation could regulate the security firms to provide better information** and encourage them to work together to find common solutions.

The security forces should work together in areas currently defined by insularity so that they pool their knowledge and resources in the battle against cybercrime. A similar pooling needs to take place at an international level. Cybercriminals operating in weak states need to be tackled through a major effort from multilateral agencies and the more capable law enforcement bodies.

In higher education, **research initiatives should also be genuinely multidisciplinary**, to include, for example, criminology, development studies,

economics (finance, micro-, macro-), IT studies, innovation studies and, even, strategic studies.

In the UK the prevailing financial crisis has required a virtual takeover by the government of key banks. **The government should use its new powers to compel the financial sector to become more transparent over the scale and nature of the threats from cybercrime** – there is a concern that banks are telling the outside world less than they actually know, not just about threat but also about potentially inconvenient counter-measures.

Our research indicates that there is no technical fix available. And no external agency can prevent all individual lapses in personal security. Instead, responses are required at all the levels identified above to minimise the risks.

National priorities in relation to cybercrime are now becoming urgent, not least because of the 2012 London Olympics. Data from the Beijing, Athens and Sydney Olympics graphically indicate how the Olympic hosts have become more vulnerable to cybercrime attacks.

The UK needs to act quickly to avert a massive international cybercrime embarrassment during the run-up to London 2012.

Contents

Executive Summary **2**

1 Cybercrime: definition and facts **10**

1.1 Definition **10**

1.2 Sources of knowledge of cybercrime **12**

1.3 Credit card fraud trends **16**

1.4 Identity theft trends **20**

1.5 Global distribution of cybercrime **28**

2 Digital ecosystem **37**

2.1 The cybercrime value chain **39**

2.1.1 Mapping the cybercrime value chain 42

2.1.1.1 Detecting vulnerabilities 44

2.1.1.2 Infection and distribution 46

2.1.1.3 Exploitation 48

2.1.2 Linkages between cybercriminals 49

2.1.3 Governance 52

2.1.4 Upgrading 54

2.2 Capabilities and specialisation **58**

2.2.1 Capabilities and specialisation for data harvesting 60

2.2.2 Capabilities and specialisation in the exploitation of information 69

2.3 Cybercrime business models **73**

2.3.1 Offline business models 74

2.3.2 Hybrid business models 75

2.3.3 Internet-based business models 76

3 Conclusions and recommendations **80**

3.1 The future trends for cybercrime **80**

3.1.1 The international level 82

3.1.2 The national level 83

3.1.3 The individual/institutional level 86

3.2 Recommendations **87**

Appendix **92**

Acknowledgements **97**

"I have ways of making money that you know nothing of."

— John D. Rockefeller

1 Cybercrime: definition and facts

1.1 Definition

Cybercrime covers a wide range of activities relating to the use of information technology for criminal purposes.

Criminals have always been alive to the possibilities of new technologies. The modernisation of 'traditional' crimes such as drug trafficking, terrorism, money laundering and extortion through the frequent incorporation of computer and mobile technologies is well known. Alongside the structural rigidity of old crime, criminal organisations are forever pioneering and seizing opportunities for new illegal enterprises made possible by the Internet and the continuing growth of electronic commerce – this type of innovation now represents the cutting edge of global criminal activity. These new opportunities require new skills but also hold out the potential for greater illicit profits. Cybercrime thus represents both the growing sophistication of existing criminal behaviour and the emergence of new types of illegal activity.

Although illegality is inherent to the concept, cybercrime it is not a legal term and its definition and coverage continuously evolve with advances in communication technologies (from computer crime to electronic and virtual crime). Cybercrime describes all kinds of crime perpetrated on new telecommunications networks, in which computers or computer networks are a tool, a target, or a locale of criminal activity.[2] By this definition cybercrime takes many forms, depending on its final purpose and means, and classifications are as varied as the number of studies on the subject.[3] In this report

[2] Adomi, E.E. (2008), Security and Software in Cybercafes, Idea Group Publishing.

[3] Numerous definitions for cybercrime can be found in the literature. We have adopted the one provided by David Wall in his thought provoking book on the subject because of its useful recognition of the informational, global and networked characteristics, which helps to locate the type of crimes with the technologies that facilitate them. Wall's definition is highly compatible with the innovation studies approach which we have adopted for this study. Wall (2007): Cybercrime: The Transformation of Crime in the Information Age, Polity Press, UK.

we focus on financial cybercrime. Other types of cybercrime such as offences against the person (cyberstalking, harassment, blackmailing), computer misuse (denial of service[4] and software piracy), and distribution of illicit material (child pornography and promotion of activities amongst paedophiles), are beyond our scope.

What is it?

"Cybercrimes are criminal or harmful activities that are informational, global and networked and are to be distinguished from crimes that simply use computers. They are the product of networked technologies that have transformed the division of criminal labour to provide entirely new opportunities and new forms of crime which typically involve the acquisition or manipulation of information and its value across global networks for gain. They can be broken down into crimes that are related to the integrity of the system, crimes in which networked computers are used to assist the perpetration of crime, and crimes which relate to the content of computers."

Source: David S Wall (2007). Cybercrime, Polity Press Cambridge, p221.

We focus specifically on credit card fraud and identity theft.[5] The choice of these two often interrelated cybercrimes is deliberate because they share with legitimate businesses the ultimate goal of financial profit, allowing us to apply business and innovation theory to understand their dynamics. These examples also help illustrate some of the more general problems facing law enforcement agencies charged with dealing with the problem. Despite this being a phenomenon involving the use of information across borders, there is no uniformity of legislative approach. This has led to an extremely permissive cybercrime environment in some countries which is of great concern to many 'stakeholders'.

Earlier research has typically been by criminologists, information technology specialists, private security firms, the financial services sector and journalists. Although, as we shall see, innovation is at the heart of these cybercrime activities, those involved in the field

[4] There have been several well publishes attacks on gaming website which effectively close down the sites until a ransom has been paid.

[5] We use the term 'credit card fraud' to encompass all forms of fraud involving credit, debit and charge cards.

of innovation studies have had little to contribute thus far.[6] In this report we explore whether innovation perspectives, insights and responses could increase our understanding of cybercrime and help to tackle it.

1.2 Sources of knowledge of cybercrime

It is often said that what cannot be measured cannot be managed. Despite the abundance of various types of cybercrime-related statistics, the lack of consensus on reliable measures and methodologies remains a matter for public concern.

Figures on the nature, magnitude and impact of credit card fraud and identity theft are far from straightforward. There have been plenty of recent estimates and forecasts. However, they employ different methods of data capture and analysis which are not always clearly explained. As a result, interpretations of statistics vary widely, as do the assessments of the effectiveness of responses and directions for future prevention. Most of our interviewees counselled that cybercrime figures need to be taken cautiously.[7]

Many organisations regularly estimate the extent of cybercrime, providing data on security threats, victimisation, financial losses and breaches in confidentiality. Each organisation includes and excludes different things which make comparisons difficult. The need for standardised measures has been recognised by both the private sector and Parliament.[8] However, the shortage of official data and a baseline against which to

[6] A notable exception has been the series of reports commissioned by the Foresight programme of the Office of Science and Technology in 2004 under the banner of the Cyber Trust and Crime Prevention project. See http://www.foresight.gov.uk/OurWork/CompletedProjects/CyberTrust.

[7] For instance Richard Clayton, University of Cambridge, stressed the importance of analysing and understanding the data in order to design effective solutions for specific cybercriminal activities (such as phishing) and avoid getting to inadequate conclusions and recommendations. Interview conducted on the 21st November 2008. Differences in published data reflect the existing differences in the conception of cybercrime by the various interested parties or 'stakeholders' of criminal activities, namely academic researchers, IT experts, law enforcement agencies, the financial services industry, retailers and the general public.

[8] The House of the Lords Science and Technology Select Committee report on personal Internet security claimed that "While the incidence and cost of e-crime are known to be huge, no accurate data exist", and recommended "[…] that the Government establish a cross-departmental group, bringing in experts from industry and academia, to develop a more co-ordinated approach to data collection in future. This should

measure all other statistical outputs still remains a major issue in understanding cybercrime.[9]

Here are some of the conclusions provided by the main existing sources:

Trends on ***information security threats*** are published regularly by security firms in what are generally named 'white papers' and technical reports, although they might be better described as commercial intelligence bulletins.[10] These reports provide useful updates on the latest threats and trends and are mainly oriented to their potential clients – businesses and the public. Their statistics need to be read cautiously since they will inevitably be shaped by different methodologies and may be linked to the marketing of protection packages offered by the different security companies. This is also why these reports often contradict each other.[11] Additionally, the accuracy of their statistics has been questioned, not least as research that indicates exponential and dramatic growth trends can do much to aid sales of security software.[12]

Figures on ***victimisation*** are collected by the Internet Crime Complaint Center (IC3),[13] a joint operation between the FBI and the US's National White Collar Crime Center.[14] IC3 records international complaints about cybercrime, though most come from within the US. In the UK, the National Fraud Reporting Centre (NFRC) is expected to become operative during 2009, as part of the recently established Police Central e-Crime Unit (PCeU). The NFRC will, in due course, offer a single contact centre for the public to report all frauds, including those online.

---

include a classification scheme for recording the incidence of all forms of e-crime". House of the Lords Science and Technology Committee, 'Personal Internet Security', 5th Report of Session 2006–07.

[9] Wall, D. (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press, UK.

[10] Some of the most widely quoted in the news and research papers include those from Symantec, Sophos, MacAfee, Kaspersky, MessageLabs, Websense and Finjan. The term 'white paper' does not refer to a government policy document.

[11] For instance, Kaspersky report (2005) predicted the gradual change in type of attacks moving away from targeting end users to direct attacks on sites and site owners with valuable information for cybercriminals. Meanwhile, Finjan (2007) reported that the nature of cybercrime has changed dramatically in the last 10 years and criminals have started targeting the user and not the system. Kaspersky (2005), 'The Changing Threat: from pranksters to professionals'; Finjan (2007), Web Security Trends Report - Q3/2007.

[12] John Leyden, "Lies, damned lies and anti-virus statistics", The Register, 16th January 2002.

[13] See www.ic3.gov.

[14] See www.nw3c.org.

Get Safe Online[15] estimates the number of victims from Internet-related fraud, and the extent of prevention and use of the Internet by businesses and the public. Data on reported victims on ID theft is provided by CIFAS,[16] the UK's Fraud Prevention Service. CIFAS figures of reported cases on ID theft and impersonation are often cited in UK publications. Additionally, Experian,[17]a global information services company, collects data on the ID fraud victims seeking their services since 2003 and publishes annually a Victims of Fraud Dossier.

The self-reporting British Crime Survey[18] and the Offending, Crime and Justice Survey,[19] cover fraud and technology offences and the Identity Fraud Steering Committee (IFSC)[20] was also set up by the UK Home Office in 2003 to identify and implement measures to counter identity fraud.

Financial losses from cybercriminal activities are reported by APACS (Association for Payment Clearing Services), the UK payments industry association.[21] APACS is the industry voice on a wide range of topics and the UK industry representative in Europe. Among other functions, APACS forecasts payment trends, conducts market research, carries out lobbying activities and collates industry statistics. APACS data on the financial costs of credit card, cheque and online banking fraud are widely cited and generally considered as an official reference that currently bears the standard. However, during our interviews, several concerns were raised that the Association may be underestimating cybercrime.[22] The IFSC has regularly estimated the cost of identity

[15] Get Safe Online is a campaign to raise awareness on Internet security for UK individuals and businesses. It a joint initiative between HM Government, the Serious Organised Crime Agency (SOCA), HSBC, Microsoft, Cable & Wireless, PayPal and Symantec, that started in 2004. See http://www.getsafeonline.org.

[16] See www.cifas.org.uk/. CIFAS has 270 members spread across many sectors that share information about identified frauds.

[17] See www.experian.com.

[18] See www.homeoffice.gov.uk/rds/bcs1.html.

[19] See www.homeoffice.gov.uk/rds/offending_survey.html.

[20] See www.identity-theft.org.uk/.

[21] See www.apacs.org.uk/. APACS has 31 members, principally global and high street banks, building societies and credit card issuers.

[22] APACS amalgamates the figures received from its 31 members and no figures for individual banks are published. Some interviewees raised the possibility that these figures may be underestimations as it is

fraud. Their methodology is still being developed, but differs from that adopted by the UK Cabinet Office.[23]

Information on ***data losses and security breaches*** is generally reported in the news and IT security online journals, although some organisations are also dedicated to the collection of this type of data. For instance, the DataLoss database[24] documents reported data loss incidents worldwide. In the UK, the Department for Business, Enterprise & Regulatory Reform (BERR, now the Department for Business, Innovation and Skills)[25] also conducts a regular survey of Information Security Breaches.

Other independent initiatives offer regular updates, trends and general information on specific types of cybercrime techniques, such as: the Anti-Phishing Working Group,[26] focused on activities that direct people to fraudulent websites through phishing, pharming and e-mail spoofing; or the Spamhaus Group,[27] which tracks and publishes information about Internet spammers as well as about spam gangs and services.

Despite the abundance of cybercrime-related figures, the lack of consensus on measures and methodologies remains a matter for public and professional concern.[28] Different organisations have their own means for collecting data. Sometimes these come directly from reports and complaints made by individuals and firms. In other cases, global and national figures are statistically suspect extrapolations from observations extracted from honeypots,[29] or relatively small populations.[30] It is important to recognise these

---

perceived to be in the banking industry's interest to deflate cybercrime fraud figures so as to allay customer fears.

[23] See www.identity-theft.org.uk/cms/assets/Cost_of_Identity_Fraud_to_the_UK_Economy_2006-07.pdf.

[24] See http://datalossdb.org/.

[25] See www.berr.gov.uk/.

[26] See www.antiphishing.org.

[27] See www.spamhaus.org.

[28] Wall, D. (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press, UK; Fafinski, S and Minassian, N (2008), "UK Cybercrime Report", GARLIK.

[29] A honeypot is a computer or a network of machines set up to look like a poorly protected system but which records every attempt to compromise it. Although they are useful to identify the way intruders operate, the activity recorded in honeypots often misrepresents the overall incidence of a certain type of attack since most sophisticated malware is designed to avoid repetitive exposure to honeypots.

[30] For instance, Symantec reported in 2008 a figure of £3.35 billion as the scale of credit card fraud by multiplying the average amount of fraud perpetrated on credit card fraud by the millions of credit card details

limitations. Estimating cybercrime still remains an inexact science and all statistics in this field should be treated with caution.

1.3 Credit card fraud trends

High frequency of credit card transactions and the wider range of available methods of payment are rapidly increasing the incidence of credit card fraud.

Credit card fraud includes the illicit use of stolen credit cards, credit card numbers, CVV2 numbers (the security code on the back) and credit card 'dumps'.[31] This information can be obtained by means such as card skimming, phishing schemes, or stealing information in personal computers or database systems (using Trojans or hacking).

According to the latest Symantec Security Threat report (2008),[32] credit card information was the most advertised category on underground economy servers, ranking the highest in terms of supplied and demanded information for 2007-08. The reasons for their high popularity are:

The frequency of credit card transactions: Consumers have almost completely switched from traditional types of payment such as cash and cheques to debit and credit cards. APACS recently reported 1.9 billion plastic card purchases made in the UK in the third quarter of 2008 totalling £93.7 billion. The number of purchases was 8.6 per cent higher than in the third quarter of 2007, and spending was 7.3 per cent higher.[33] The 'credit crunch' may slow this growth but the overall trends indicate a clear move away from paper to electronic payments.

A growing preference for online transaction: The number of adults shopping online has trebled from 2001 to the present in the UK (from 11 million to over 30 million), and these figures are consistently rising. The growth in e-commerce increases the

---

the company observed in underground markets. This figure can be easily questioned, since it does not account for the number of cards that were cancelled or inoperative, or the high variation of the amounts stolen from credit cards. Estimated by Symantec (2008), "Symantec Report on the Underground Economy".

[31] 'Dump' is a slang word for stolen credit card information and usually contains among other things: name and address of cardholder, account number, expiration date, verification/CVV2 code.

[32] Symantec (2008), "Symantec Report on the Underground Economy", July 07–June 08.

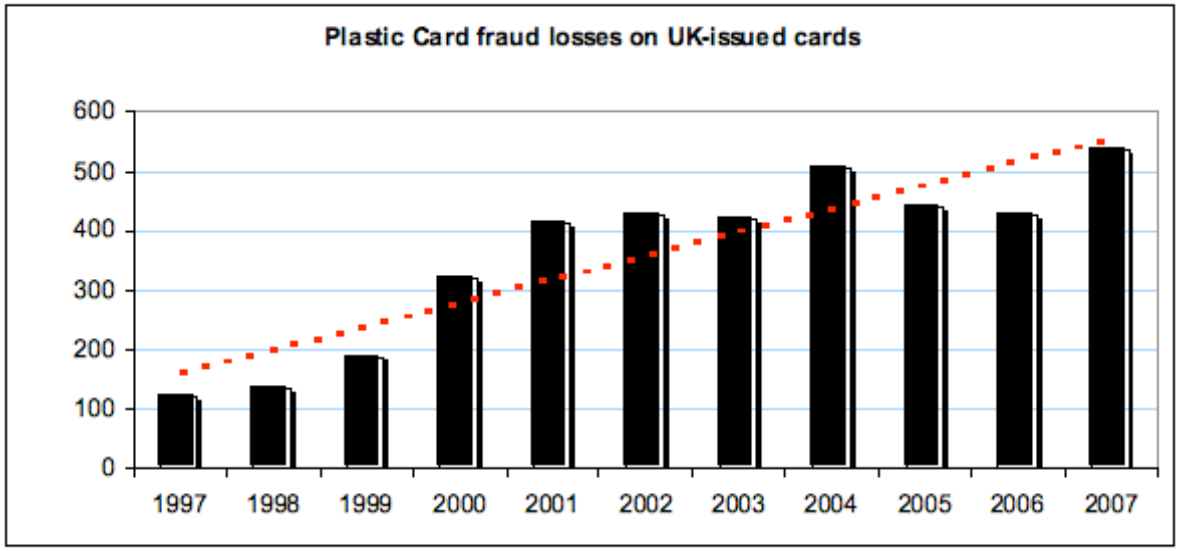
[33] This increase is mostly materialised on debit cards, which accounted for 73.8 per cent of all plastic card purchases compared with 72.0 per cent in the third quarter of 2007.

opportunity for online theft of credit card information. Internet sales by UK businesses reached £163 billion in 2007, an increase of over 30 per cent on the 2006 figure of £125.2 billion.[34]

The greater frequency of credit card transactions through Pin Entry Devices, online or phone payments increases the opportunities for criminals to capture data. These later are supplied on underground servers.[35] As a consequence, credit card fraud has increased rapidly, reaching £535.2 million in 2007 in the UK alone, according to APACS. International credit card fraud for 2007/2008 has been estimated at £3.35 billion.[36]

Figure 1 shows that the latest increase in UK card fraud follows a temporary slowdown during 2005 and 2006, which coincided with the introduction of chip and pin technology. Average growth has been 16 per cent a year since 1997.

Figure 1



Source: Calculated from APACS, "Fraud: the facts" (2008).

[34] The Office for National Statistics (ONS) database.

[35] Symantec (2008) "Symantec Report on the Underground Economy", July 07–June 08.

[36] Estimated by Symantec (2008), "Symantec Report on the Underground Economy", July 07–June 08. However the accuracy of this figure can be questioned since it was calculated by multiplying the average amount of fraud perpetrated on a stolen card, $350 (£234), by the amount of credit card details Symantec observed being offered for sale, including those potentially invalid or cancelled.

Credit card fraud takes place mostly online. The categories of credit card fraud that show the fastest growth include a substantial online component. This is reflected in the increase of card-not-present fraud (CNP), counterfeit cards[37] and card ID theft, since these types of fraud are more likely to occur online. Such methods are becoming more important than the use of lost or stolen cards, or theft from the mail.[38]

Figure 2 shows that these three categories of credit card fraud have proliferated in the last decade, reflecting the rise in online transactions. Fifty-four per cent of card fraud was on CNP operations, the fastest growing form of credit card fraud, with average growth rates of 40 per cent per year from 1997 to 2007. APACS estimated that in the UK, the share of Internet/e-commerce fraud on CNP activities was about 73 per cent of the total in 2006 (£154.5 million). This figure rose by 32 per cent from 2005, when Internet losses were £117 million and accounted for 65 per cent of CNP losses.[39] Using fraudulent credit card data for online purchases can be easy and fast, as a final sale does not require the card or the cardholder to be present. Online purchases can later be sold for cash.[40]

Fraud based on counterfeit cards temporarily fell from 2004 to 2006, perhaps due to the introduction of chip and pin technology, but it picked up in 2006 to 2007 – at a 46 per cent growth rate as cybercriminals discovered ways of outsmarting and circumventing these preventative technologies. Chip and pin technology was described as an 'extremely secure' method of payment by representatives of banks and retailers.[41]

[37] This category can involve undertaking old style fraud, by skimming (ATM skimming, manipulated Pin Entry Devices or a range of other more sophisticated techniques).

[38] CNP fraud involves the use of stolen card details to pay for goods and services over the Internet. Card ID theft occurs when a criminal uses a fraudulently obtained card or card details, along with stolen personal information, to open or take over a card account in someone else's name. Counterfeit card fraud involves copying the information of the magnetic stripe in the card to forge a fake card that can be later used in ATMs or to make purchases. As defined by APACS (2008): "Fraud: The Facts 2008".

[39] APACS, "Fraud: the facts" (2008).

[40] For more information on this aspect see the section of this report on cybercrime value chains.

[41] Sandra Quinn, director of corporate communications for APACS in 2005 noted that: "We don't think they can use fake machines because the machines themselves are engineered to read the chip so they must be reading the chip very carefully"; "Chip and pin security warning", BBC News, available at http://news.bbc.co.uk/1/hi/business/4108433.stm. This was reiterated during a recent interview with a senior APACS staff member in 2008.

However, the recent increase in fraud, based on counterfeit cards which still represent nearly one-third of the total credit card fraud in the UK indicate that it was simply a matter of time before criminals found a way around it.[42]

Card ID theft has increased at an average rate of 10 per cent per year, although this more modest increase may reflect the greater risks involved compared with other types of credit card fraud. For instance, large fraudulent bank transfers or smaller but uncharacteristic activities can quickly alert the credit card issuer allowing the transfer to be suspended and tracked. Cards can also be automatically blocked and transfers prevented.[43]

The rapid growth in cybercrime comes at a time when more traditional crimes are falling. Both police recorded crime[44] and the British Crime Survey (BCS) 2008[45] show a steady recent decrease in violent crime – such as violence against the person, sexual offence and knife or gun-induced robbery - falling by 10 per cent from 2006/07 to 2007/08.[46] The latest British Crime Survey estimated that the risk of becoming a victim of crime fell from 24 per cent in 2007 to 22 per cent in 2008, representing nearly a million fewer victims.[47] Even the total figure for fraud and forgery has reduced,

[42] Interview with IT security experts at the Computer Laboratory, University of Cambridge, 21st November 2008. An interview with Detective Inspector Roy West of the City of London Police referred to the manufacture of ATM component parts in Eastern Europe with pinhole cameras and skimming devices which can be fitted in seconds.

[43] For example, when cards are used in high risk countries, such as Sri Lanka, they are automatically blocked until the user calls in to confirm and verify that the card is still the property of the owner.

[44] Crime data are collected from police forces on a monthly basis for each crime within the notifiable offence list. Notifiable offences include all offences that could possibly be tried by jury (these include some less serious offences, such as minor theft that would not usually be dealt with this way) plus a few extra closely related offences, such as assault without injury.

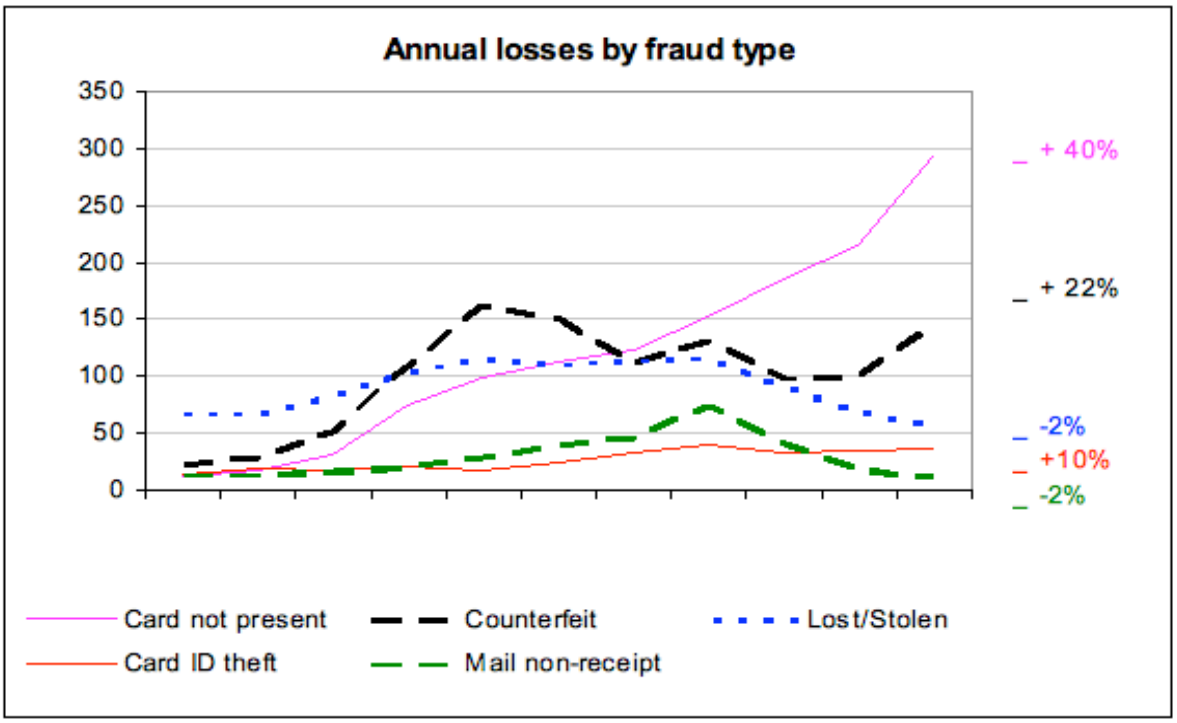
[45] The findings in the British Crime Survey (2008) are based on 46,983 face-to-face interviews conducted by BMRB Social Research between April 2007 and March 2008.

[46] However, the figures of total crime incidence differ considerably between these two sources, since the BCS total for 2007/08 was 10.1 million crimes; while police recorded crimes were about 5.0 million. Home Office (2008): "Crime in England and Wales 2007/08: A summary of the main findings".

[47] However, the risk of victimisation varies by personal and household characteristics and by crime type. Home Office (2008): Crime in England and Wales 2007/08: A summary of the main findings.

according to the police records, from 199,700 offences in 2006/07 to 155,400 in 2007/08 – a 22 per cent decrease.[48]

Figure 2



Source: Calculated from APACS, "Fraud: the facts" (2008).

1.4 Identity theft trends

Identity theft is on the rise, but so are the detection techniques. Increasing data breaches and the widespread social networking websites could lead to the growth of identity fraud, since they provide a platform for cybercriminals to access large amounts of personal information.

Identity theft is the misappropriation of somebody else's personal details, without their knowledge or consent. However, ID theft is not in itself an offence in the UK, and

[48] These offences were modified by the Fraud Act 2006 which came into force on 15 January 2007. For cheque and credit card fraud counting changed from per fraudulent transaction to per account basis from 15 January 2007. From 1 April 2007 these offences were reported to a single point of contact within each police force by financial institutions. Source: Home Office (2008): "Crime in England and Wales 2007/08: A summary of the main findings".

penalties for those who make fraudulent applications (for example for passports) are very small.[49] Identity fraud occurs when the misappropriated identity is actually *used* in criminal activity, to obtain goods or services by deception, generally for financial gain. This is a criminal offence in the UK.

ID theft generally combines online and offline methods. Online methods include stealing personal information stored in computer databases (using Trojans or hacking); or through phishing, vishing and pharming (see glossary). Offline methods include intercepting bills and bank documents from the post and rubbish bins. These techniques allow cybercriminals to obtain Social Security numbers, bank or credit card account numbers, phone numbers, addresses, birth dates, usernames and passwords; all information that criminals can use to perform illicit transactions with another person's identity.[50] According to CIFAS, the top three false or stolen documents used by fraudsters attempting identity fraud in 2006 were: utility bills, passports and bank statements.[51]

The full scope of the impact of ID fraud is hard to measure, since this type of crime can take months to be noticed by the victim and be reported. Available financial compensation and legislative measures do not account for the cost in recovering the reputation of the victims (particularly their credit rating). The impact of identity fraud varies substantially. CIFAS reported that it can take between three and 48 hours of work for a typical victim to sort out their life and clear their name but in cases of 'total hijack' where many of their details are stolen it can take 20-30 different organisations, over 200 hours and up to £8,000 to recover from the consequences of the fraud. [52] However, financial institutions and lending organisations are often considered to be the real

[49] Cabinet Office, (2002), "Identity Fraud: a study", p.4.

[50] With even the most basic information, a criminal can either take over another person's existing financial accounts or use somebody's identity to create new ones. Common fraudster activities include withdrawing funds from your accounts, charging purchases to your credit cards, opening up new telephone accounts or taking out loans in your name, all of which can have a damaging effect on the victim's credit rating.

[51] CIFAS website: www.cifas.org.uk.

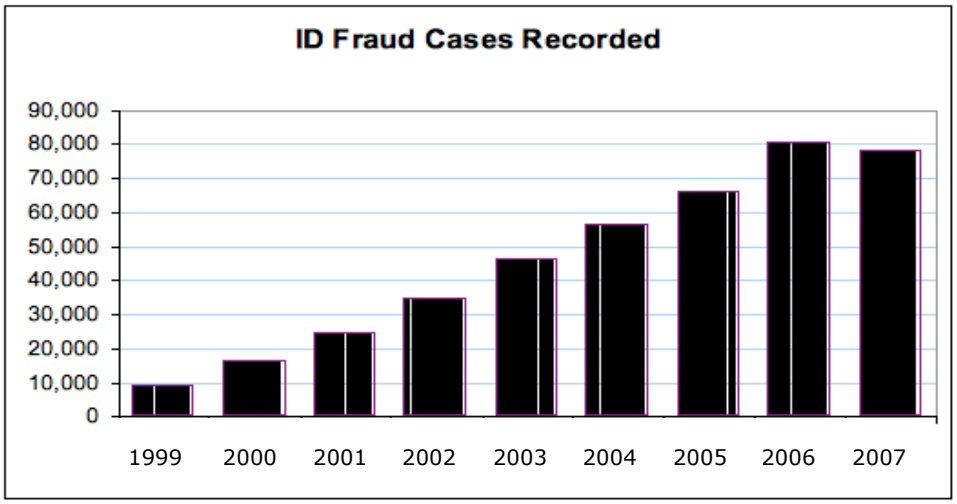
[52] See www.cifas.org.uk/.

victims since they bear the direct financial costs of ID fraud – although these may well be passed on to customers in higher service charges.[53]

The risk of perpetrating ID fraud appears to be relatively low, since most cases are not reported to the police. An Experian study in 2007 indicated that ninety per cent of identity fraud cases were not reported to the authorities and only six per cent of the reported cases led to a prosecution. [54]

In 2007, CIFAS reported 77,500 victims of identity theft and identify fraud in the UK. The cases reported have exponentially grown from 9,000 in 1999 to 80,000 in 2006, which represents an annual increase of over 30 per cent, though there was a small 3 per cent fall between 2006 and 2007. According to Experian, directors of medium and large companies and high income earners (more than £50,000 a year) are more likely to become victims of identity fraud – between three and five times higher propensity – than the average UK resident.[55, 56]

Figure 3



[53] Any such compensation to the individual needs to be fought for through the civil courts. This is likely to continue to be the case until legislation is introduced specifically to outlaw identity theft, as in the USA; www.cifas.org.uk/.

[54] Experian (May 2008), "Victims of Fraud Dossier". Based on the 6,000 victims that sought their services in 2007.

[55] Heera, S (2008), "Directors of larger dealerships at significant risk of identity theft, warns Experian", New Release, Experian.com. See http://press.experian.com/documents/showdoc.cfm.

[56] Making London an obvious hotspot for ID fraud.

Source: Elaborated from CIFAS online, UK's Fraud Prevention Service. www.cifas.org.uk

Available statistics indicate that identity fraud is on the rise. Attempted identity frauds rose 21.5 per cent from 2005 to 2006 and 12 per cent from the first half of 2007 to 2008.[57] Moreover, from 2007 to 2008 CIFAS members reported a 159 per cent increase in account takeover fraud.[58] However, detection and prevention techniques seem to be increasingly efficient, since the number of attempted ID frauds detected before an account was opened increased during 2006 by almost 40 per cent. This means that a higher proportion of the victims whose identities had been compromised never had any money stolen from their accounts, or products taken out in their name.[59]

While the impact of identity fraud is not easy to gauge,[60] the Identity Fraud Steering Committee (IFSC)[61] estimated the cost of ID fraud to the UK economy at £1.2 billion in 2007, the equivalent to £25 per person. Major updates in accounting and calculation methodology make this figure incomparable with previous estimates of £1.3 billion in 2002 and £1.7 billion in 2006 from the Cabinet Office.[62]

Other reports suggest that identity fraud activity may only represent a small fraction of total online fraud. For instance, the 2008 Symantec security threat report[63] indicated that identity theft information for sale, as advertised on underground servers, represented only 7 per cent of all the categories for sale in 2007, and 10 per cent of the type of information most demanded by cybercriminals. Since full identities consist of a combination of multiple pieces of information (name, address, mother's maiden name,

[57] According to CIFAS; see www.cifas.org.uk.

[58] When a fraudster impersonates an individual in order to 'take over' his/her bank account.

[59] See www.cifas.org.uk.

[60] Cabinet Office, (2002), "Identity Fraud: a study".

[61] The Identity Fraud Steering Committee (IFSC) was set up by the Home Office in 2003 to work with public and private sector organisations to identify and implement cost effective measures to counter identity fraud. See www.identity-theft.org.uk/committee.asp.

[62] The initial figure added overlapping figures from CIFAS and APACS, and included other payments not directly related to identity fraud. Home Office Identity Fraud Steering Committee (IFSC), "New Estimate of Cost of Identity Fraud to the UK Economy", available at http://www.identity-theft.org.uk/cms/assets/cost of identity fraud to the UK economy2006-07.pdf.

[63] Symantec (2008), "Symantec Report on the Underground Economy", July 07–June 08.

e-mail addresses, etc), their low supply might be a direct result of the difficulty in compiling such information.

However, other continuous data breaches are also exposing personal information on a large scale. Seven hundred data breaches were reported worldwide from 2007 to 2008, which resulted in 200 million identities exposed.[64] This figure represents an increase of 83 per cent compared to the previous year. In the UK, numerous Government data breaches have made the news.[65] But the problem affects all sectors: one survey has reported that 55 per cent of British companies have lost data in 2008,[66] and 96 per cent of the UK companies with more than 500 employees reported a computer related security incident in 2007.[67] The proliferation of larger centralised databases threatens more personal data being lost or abused.[68]

Despites this, the UK government announced in 2008 that it will not be implementing a data-breach notification law, similar to laws in many US states.[69] The importance of reporting private data breaches has been a recurrent critical concern raised by the majority of our interviewees, including IT security firms, IT experts, academics and the police.[70] This was also the view of the House of Lords Science and Technology committee in their personal security report: "a data security breach notification law would be among the most important advances that the UK could make in promoting personal Internet security". As there is no UK legislation that demands the publication of private breaches, the full extent of the problem remains unknown.

[64] See http://datalossdb.org/.

[65] For example, HM Revenue and Customs (HMRC) lost 25 million child benefit records in November 2007. In January, the Ministry of Defence lost a laptop containing the details of over 1 million people. In May 2008, the Department for Transport lost the data of three million learner drivers. More recently, in November 2008 the Ministry of Justice admitted it had lost 45,000 people's details throughout the 2008.

[66] Leo King, "Over half of UK firms have lost data", Computerworld UK, 13/10/2008; available at http://www.computerworld.com.au/index.php/id;1869348852;fp;39;fpid;26027.

[67] Department for Business, Enterprise & Regulatory Reform (BERR): Information security breaches survey (2008).

[68] Speech by Richard Thomas, information commissioner, in October 2008. In Alan Travis, "Bigger databases increase risks, says watchdog", The Guardian, Wednesday 29 October 2008; available at http://www.guardian.co.uk/technology/2008/oct/29/data-security-breach-civil-liberty/print.

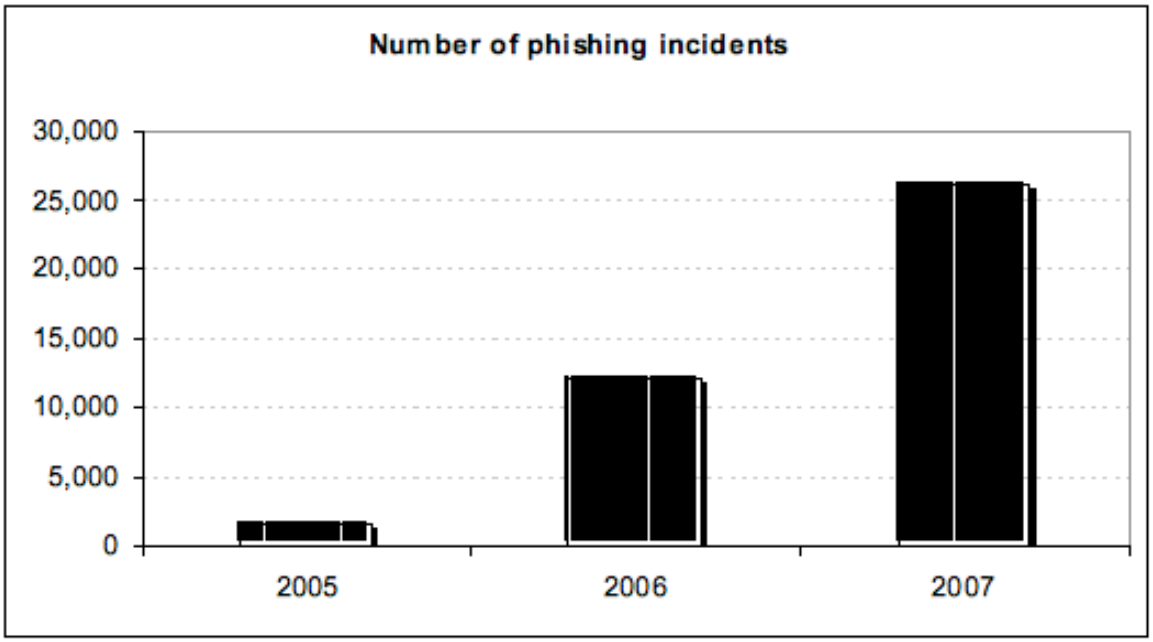
[69] It is already mandatory for public-sector organisations to report any significant actual or potential losses of data to the Information Commissioner's Office (ICO).

[70] Interviews conducted from November 2008 to April 2009.

The rise of online and telephone banking have also increased opportunities to obtain personal data through phishing and vishing. In 2006, 24 million UK adults used remote banking to access their main current account, and APACS anticipates that by 2014 over two in three adults will be using remote banking.[71] The majority of these users use only the Internet to access their main account. The active transit of online banking has resulted in total losses of £33.5 million in 2006 for online banking fraud from scams such as phishing and Trojans, an increase of 44 per cent from 2005.[72]

However, these figures are expected to rise in the near future with the higher incidence of phishing attacks and the widespread presence of password stealing malware. In the UK, APACS reported phishing attacks have grown from fewer than 2,000 in 2005 to nearly 14,000 in 2006 to nearly 26,000 in 2007.[73]

Figure 4



Source: APACS, (2008).

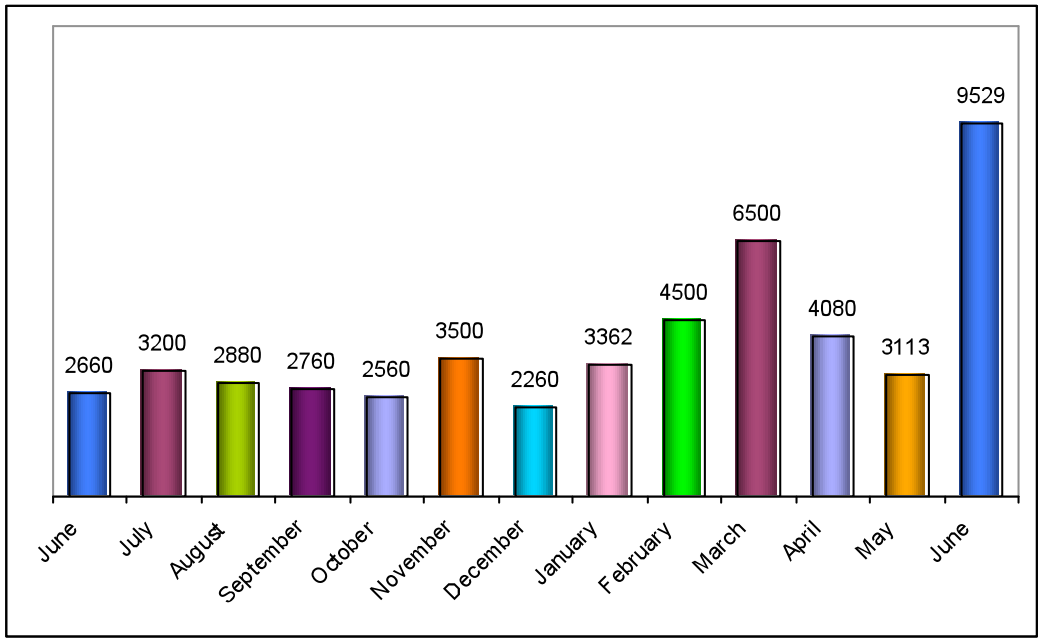
[71] APACS (2007), "Payment facts", at www.apacs.org.uk/media_centre/documents/070522_FINAL_OnlineBankingFactPack.pdf.

[72] APACS, (2007), "Fraud the facts".

[73] BBC News, (2008), "Bank phishing on the rise," 24th July. A phishing 'incident' is an incident where the bank or banking service provider is compelled to react to a phishing problem and records it as such.

Internationally, a recent report from the Anti-Phishing Working Group indicates that the amount of password-stealing crimeware multiplied almost fourfold from 2007 to 2008 – from 2,660 in June 2007 to 9,529 in June 2008.[74] The financial sector is the most targeted by phishing attacks, followed by auctions and payment services sites. However, the Anti-Phishing Working Group also reported a fast growth of targeted attacks directed to social networking sites such as MySpace and Facebook in addition to tax agencies.

Figure 5: Password stealing malicious websites 2007/2008



Source: Anti-Phishing Working Group (2008)

The possibilities offered by social networking websites are increasingly a source of major concern. Facebook and MySpace have become phenomenally popular worldwide[75] making them attractive places for cybercriminals because: (1) they allow the spread of malware, spam and scams on a massive scale, (2) they are gradually becoming a

[74] Anti-Phishing Working Group (2008): "APWG Phishing Activity Trends Report", Q2 2008.

[75] Facebook was identified in 2008 as the largest social network in UK with 45 per cent market share, followed by Bebo and MySpace, while MySpace remained ahead in the USA with 72 per cent market share. Cahill, J, (2008). New Release, Experian.com. See http://press.experian.com/documents/showdoc.cfm.

recruitment marketplace for cybercriminals and (3) they contain vast amounts of personal information that can be used for identity theft.[76]

MySpace or Cybercrookspace?

Cybercrooks are increasingly using MySpace and Facebook to recruit people, network, spread malware, and steal personal information. Cybercriminals are exploiting the popularity of social networking sites to steal identities or craft more personalised fraud attempts. Facebook, which has exploded in popularity in the UK in recent months, allows people to post detailed, personal information about themselves from their date of birth to the schools they attended – precisely the information that banks ask for as security questions. Someone's mother's maiden name, or place of birth, is now so easily available to become almost redundant. Tim Pie, at HSBC, said: "There will come a time when that sort of identification will become a thing of the past."

In August 2008 Kaspersky Lab discovered two worms that had been specifically designed to target MySpace and Facebook. Also, a federal judge has ordered a Canadian man to pay Facebook $873 million for blasting members of the social networking site with spam.

Sources: Dan Kaplan, (2008), articles in http://www.scmagazineus.com/.; Harry Wallop, Consumer Affairs Correspondent (4th July 2007), Fears over Facebook identity fraud, The Telegraph.

[76] Facebook adopted open innovation in 2007 by releasing Facebook Platform for application developers. Since then, thousands of third-party applications on Facebook have become available, which allows the developers to access information from those Facebook users that install these applications. Tightening security to protect the privacy and personal information from Facebook users would contradict the principles of open innovation, based on sharing information.

1.5 Global distribution of cybercrime

Cybercrime is a global industry but the combination of poor economic opportunities and high skills is driving many developing regions to surface as major players in cybercrime.

Cybercrime has experienced a higher degree of globalisation[77] perhaps due to its ability to gravitate to permissive environments – countries with minimal legal restrictions – and the nature of the technology involved. All the published evidence and our interviews strongly confirmed that cybercrime is a global issue, and international collaboration among the cybercriminals is expected to grow in the future. The global nature of the Internet facilitates participants from all locations, while law enforcement authorities struggle to unify their laws on cybercrime.

The increasingly even distribution of the required skills to perpetrate cybercrimes, coupled with uneven prosecution procedures and legislations, are driving the fast global redistribution of the geographical location of cybercrime.[78]

Unsurprisingly, most cybercrime attacks are currently directed to the US and the UK, since they account for a high proportion of financial traffic globally. A recent report confirmed the US as the most widely targeted country in November 2008, absorbing 53 per cent of the world's phishing attacks. The UK was the second highest targeted country at 15 per cent, followed by Italy, Spain and Canada.[79] Figure 6 shows that the origin of phishing activities is also concentrated in a few international locations, namely the US, Southern Asia and Eastern Europe. Other locations, such as Brazil and India are also rapidly entering the global cybercrime scene.

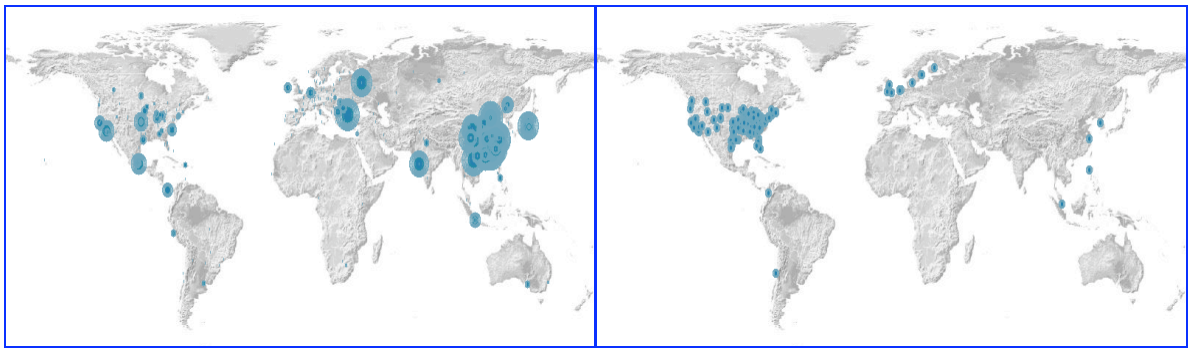
[77] Kshetri, N, (2006), "The Simple Economics of Cybercrimes", IEEE Security and Privacy, Vol. 4, No. 1.

[78] Although 34 countries initially signed the Council of Europe's Convention on Cybercrime in November 2001 many have not, as yet, ratified the convention, including the UK.

[79] RSA Anti-Fraud Command Center (November 2008): A Monthly Report from the Phishing Repository.

Figure 6: Origin and destination of phishing attacks

Origin of phishing attacks **Destination of phishing attacks**



Source: Arbor Networks (http://www.arbornetworks.com/).

Each region has its own digital ecosystem – or networks – and has developed technological capabilities according to their available skills, domestic context and local vulnerabilities. These have been characterised by some reports,[80] and can be summarised as follows.

(A) The United States is still the major generator of malware and according to the latest Symantec report it is still the country with the most underground servers (hosting 41 per cent of the total servers observed by Symantec from 2007 to 2008).[81] In 2006 the United States was reported as the top country in the world hosting web-based malware. However, other reports argue that this position has been overtaken by China in 2007.[82]

(B) Much attention is placed on China when considering the future of cybercrime. China has more than 137 million computer users, one-quarter of whom play online games, and cybercriminals are feeding on this massive interest. Chinese hackers are currently focused on developing the Trojans that lift personal information from online

[80] MacAfee, (2008), "One Internet, many worlds", Sophos Security Threats reports (2007, 2008).

[81] Symantec, (2008), "Symantec Report on the Underground Economy", July 2007–June 2008. However, the report does not provide a total number of underground economy servers on which the study is based upon.

[82] Sophos Security Threats reports (2007, 2008).

video games.[83] However, the activities and level of organisation of Chinese hackers transcends the online game industry. A 2009 report provided compelling evidence and detail of the efforts of a network of Chinese hackers – which researchers have called GhostNet – that uses a malicious software programme to steal sensitive documents, control web cams and completely control infected computers. Investigations have disclosed 1,295 hacked computers in 103 countries belonging to international institutions. The report says "GhostNet represents a network of compromised computers resident in high-value political, economic and media locations spread across numerous countries worldwide."[84] There are also concerns that Chinese groups are becoming adept at applying ransomware.[85] Of particular concern is where 'Denial of Service' (DoS) attacks are beginning to target government agencies beyond China and thereby developing the potential to use these means as a weapon of war. There are very strong suspicions that these efforts at the very least are sanctioned or involve the state.[86]

(C) Russia has traditionally been considered the original home of cybercrime, where high technical skills combine with a stumbling economy and a long tradition of organised crime.[87] Russian programmers are believed to be behind the most widely used malware-making toolkits such as Mpack and WebAttacker. Dubbed 'the mother of cybercrime', the Russian Business Network (RBN) has been linked by security firms to child pornography,

[83] Kaspersky, "Security Trends 2008". This subject has also been reported by vnunet.com, "Identity theft feeds $1 bn gaming black market", February 21 2006.

[84] Information Warfar Monitor (2009) "Tracking GhostNet: Investigating a Cyber Espionage Network".

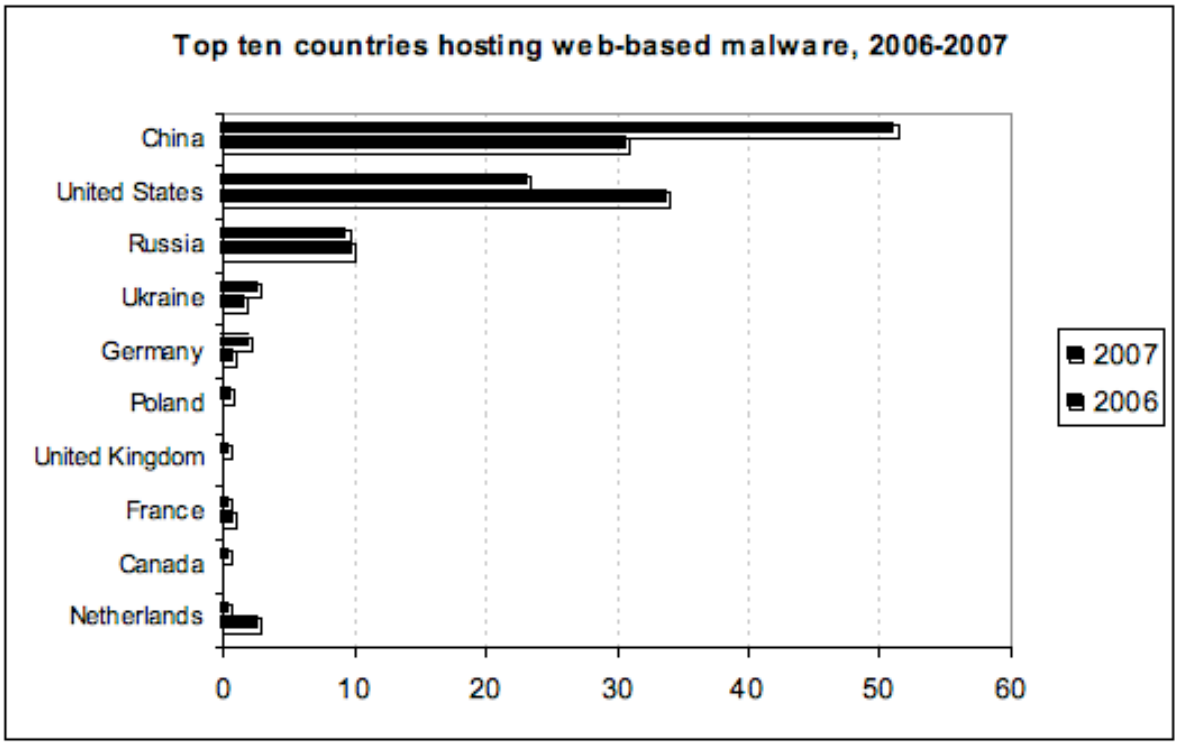
[85] Malicious software which hijacks a personal computer and locks files until a ransom is paid. The first known case in the UK was in mid-1996 when a nurse from Rochdale found her computer files locked and was notified that she would have to pay to access a password to have them unlocked (presumably by credit card). Chapman, M., (1st June 2006), Ransomware hijacks nurse's PC, vnunet.com, http://msn.vnunet.com/vnunet/news/2157359/ransomeware-hijacks-nurse-pc, accessed 3rd December 2008.

[86] Greenemeier, L., (18th September 2007), China's Cyber Attacks Signal New Battlefield in Online, Scientific American, http://www.sciam.com/article.cfm?id=chinas-Cyber-attacks-sign, accessed 4th December 2008.

[87] In 1993, after the European Council invited Estonia, Latvia and Lithuania to apply for EU accession, the Baltic States implemented an intensive period of national and cultural reconstruction following years of encroachment from Russia, especially the penetration of Russian organised crime groups. At the centre of this purge was an attempt to stem the incursion of non-indigenous criminal influence on public-sector employers. It would seem that very early on in the evolution of the Internet, Russian organised crime became aware of its potential. After the collapse of the Soviet Union, the nascent Russian Business Network (RBN) is thought to have taken a keen interest in the IT skills that existed in the Baltic States. It also took a similar interest in the underemployed IT experts in the former Soviet Union's military, many of whom remained unpaid for months on end.

corporate blackmail, spam attacks and online identity theft, although most Russian cybercrime is directed to financial fraud, particularly through botnets (collections of compromised computers) and phishing.[88] Although its activities online have often been highly visible, relatively little is known about who is (or was) behind the RBN.[89]

Figure 7



Source: elaborated from Sophos Security Threats reports (2007, 2008).

The RBN is widely thought to have shut down or relocated in 2007. However, this does not seem to have left a void in the fast emerging world of malware designed to harvest financial information. There have been reported cases where banking authentication information data has been sent to a series of sites belonging to a Chinese network.[90, 91]

[88] Rhys Blakely, Jonathan Richards and Tony Halpin, Cybergang raises fear of new crime wave in Moscow, Timesonline.com, 10th November 2007.

[89] Symantec, (2008), "Symantec Report on the Underground Economy", July 07–June 08.

[90] The sums, usually around $50,000, are also small enough not to interest law enforcement agencies to any great extent.

Russian groups have also started to specialise in Denial of Service (DoS) attacks, particularly on online gambling sites.[92] [93]

The foray into cybercrime has not been designed as a replacement for more traditional forms of organised crime. It remains unclear which brand of activity is more important to the enduring prosperity of Russian organised crime and indeed the inter-relationship between the two strands. Given the low overhead profits associated with cybercrime against high overheads associated with traditional organised crime, cybercrime is a necessary endeavour to maintain the social and political benefits that accrue from the more visible and high profile criminal areas.[94, 95]

The amount of financial information procured by Russian organised crime groups is thought to be massive. Much of it is stored covertly on unsuspecting servers across the world.[96] Considerable though the impact has been on individual current account and credit card holders, these victims are thought to represent only about 1 per cent of the total information that is held globally and illegally.[97] Quite apart from the implications for the future, as and when this information does enter the financial domain, its very existence presents the organised crime group decision makers with an interesting choice regarding use. Effectively, at this juncture, they have opted to sell the information rather than use it directly, in order to avoid being at the point of crime. For example,

---

[91] Carr, J., (18th December 2007), 'Finjan: Chinese Cybercrime networks fill void left by Russian Business Network, SC Magazine, www.scmagazineus.com/Finjan-Chinese-Cybercrime-networks-fill-void-left-by-Russian-Business-Network/article/100002/, accessed 3rd December 2008.

[92]The actual ransoms are generally not large and usually are less than what the site would lose if service were denied for any longer than a week. Russian Mafia target online gambling sites, OnLine Casino, www.onlinecasinonews.com/ocnv2_1/article/Article.asp?id=4460, accessed 3rd December 2008.

[93]Successful Russian attempts to compromise IT networks in Georgia and Estonia point to the potency of DoS as a weapon of war. The techniques that were used were neither complex nor, allegedly, overseen by central government. In the case of Georgia, the campaign was initiated by Russian nationalists who posted the relevant software on websites, which could be downloaded by anyone so inclined to contribute to a flood of bogus requests to an Internet server that culminated in a 'Distributed Denial of Service'. (6th-12th December 2008), Marching off to Cyberwar, The Economist (Technology Quarterly), p.18.

[94] Interview with Colin Whittaker, Head of Security, APACS, London, 30th July 2008 and, 14th October 2008.

[95] As Misha Glenny's recent book consistently reflects, not all crime is about money and wealth; it is also about relative power, position and social advantage. Glenny, M., (2008), McMafia: Crime Without Frontiers, (Random House, London), p.426.

[96] Interview with Colin Whittaker, Head of Security, APACS, London, 30th July 2008.

[97] Interview with Tim Warner, Sales director and Country Manager, Finjan, Brighton, November 2008.

Nigerian criminal gangs in North America and Western Europe have made extensive use of these opportunities. There are thought to be more than 500 Nigerian organised crime groups operating in 80 countries.

From Russia with love

According to VeriSign, one of the world's largest Internet security companies, RBN, an Internet company based in St Petersburg, is "the baddest of the bad". In one sense, RBN (Russian Business Network) does not exist. It has no legal identity; it is not registered as a company; its senior figures are anonymous, known only by their nicknames. Its websites are registered at anonymous addresses with dummy e-mails. It does not advertise for customers. Those who want to use its services contact it via Internet messaging services and pay with anonymous electronic cash. But the menace it poses certainly exists. "RBN is a for-hire service catering to large-scale criminal operations," says the report. It hosts cybercriminals, ranging from spammers to phishers, bot-herders and all manner of other fraudsters and wrongdoers from the venal to the vicious. VeriSign estimates that a single scam, called Rock Phish (where gullible Internet users were tricked into entering personal financial information such as bank account details) made $150m in a year.

Source: www.economist.com (20 August 2007).

(D) More recently, Brazil has emerged as a significant player on the global cybercrime stage[98] and a "cesspool of fraud" according to one commentator.[99] The main driver that encourages young Brazilians to develop their skills is impunity – Brazil lacks any form of effective legislative framework to combat cybercrime. Another driver would appear to be cultural.[100, 101] Brazilian hackers are increasingly sophisticated, particularly in online

[98] Gibb, T., (14th September 2004), Brazil is world 'hacking capital', BBC News, http://news.bbc.co.uk/1/hi/world/americas/3657170.stm.

[99] Paul Fisher, "Brazil is cesspool of fraud", Scmagazine, October 28, 2008.

[100] Cybercriminals from Brazil are largely, it would seem, independent operators, brought together by chatrooms. Generally, they started cyberlife as hackers and graduated via the chatrooms to more lucrative pursuits. Glenny, M., (2008), McMafia: Crime Without Frontiers, (Random House, London), pp.303 – 313.

[101] Brazilian Cybercriminal are thought to be more sociable and open than their counterparts in other parts of the world and are more prepared to share data and develop knowledge collectively, albeit via anonymous

banking fraud. Malware creators are rapidly developing and adapting malware to avoid the security prevention techniques from banks. Operation Pegasus, launched by Brazilian authorities, arrested 85 people in 2005 as part of a ring planting keyloggers (software that logs people's keyboard activity) that helped the alleged criminals steal approximately US$33 million from bank accounts.[102] However by the end of 2005, Brazil still reportedly had the highest concentration of phishing-based keyloggers that target Brazilian financial institutions, using deception techniques written in Portuguese.

Since then, the number of cyber attacks has continued to escalate in Brazil, according to the country's Computer Emergency Response Team (CERT), from 68,000 in 2005 to 222,528 in 2008. Moreover, from January to March 2009 the attacks have already reached 220,000 almost the total accumulated figure for 2008. The majority of the cyber attacks are fraud-related (80 per cent of the attacks), and are mostly originated locally (93 per cent originated in Brazil).[103]

(E) Although cybercriminal activity remained low in India compared with other emerging economies, there has been a leap in cybercrime in recent years – reported cases of cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007.[104] One recent report ranked India in 2008 as the fourteenth country in the world hosting phishing websites.[105] Additionally, the booming of call centres in India has generated a niche for cybercriminal activity in harvesting data (methods further explained in section 2.2.1 below).

Cybercrime in India: harvesting data in call centres

India is the world leader in business process outsourcing (BPO). The country's top ten BPO firms hire up to 25,000 new employees per year, and financial services are one of

chatrooms. Smith, T., (27th October 2003), Brazil Becomes a Cybercrime Lab, New York Times, http://query.nytimes.com/gst/fullpage.html?res=9F02E3DA1131F934A15753C1A9659C8B63&sec=&spon=&pagewanted=2, accessed 4th December 2008.

[102] Haines, L (2005) "Brazil cuffs 85 in online bank hack dragnet: Operation Pegasus", The Register.

[103] See www.cert.br/stats.

[104] Indian Computer Emergency Response Team (CERT-In): Annual Report, 2007.

[105] Symantec (2008): Report on India cybercrime.

the fastest growing segments. However, low salaries and fast turnover in the industry might provide an incentive to make extra money through cybercrime.

Call centre cybercrime is becoming popular. A recent article in *India Daily* stated that for locals in Pune and Bangalore in India, the biggest incentive to work in a call centre is to be able to hack the bank accounts and illegally withdraw millions from bank customers. During the last five years, the number of reported cases has multiplied and undercover investigations have revealed the large flow of stolen personal data that is moved through call centres in financial services.

Amid fears of losing international customers, local companies have tightened security measures. Although these cases have been labelled as isolated cases of fraud, certain investigations have suggested that there is evidence of some operations being carefully designed and very organised.

Sources: Ahmed, Z. (2005) 'Outsourcing exposes firms to fraud', BBC News Online, 16 June; Gombar, V. (2006)'Indian call centres under threat', Rediff India Abroad, 22 July; Patel, H. (2007) 'Call center cyber crime increasing – many trying to hack into bank websites and illegally withdraw millions – one gets into police net', India Daily, 17 November.

Russia, China and Brazil are world leaders in cybercrime, with groups and individuals in India powering up to compete. Yet companies in Europe and the US are increasingly moving IT functions and software development tasks to India, Brazil, Russia and Eastern Europe in a bid to draw on their good IT skills and lower wages. This phenomena (offshore outsourcing), has raised new concerns about the security risks involved, where access to valuable financial information can provide an opportunity for different actors to enter the cybercrime business.

It is no coincidence that these are also the BRIC[106] nations that are seen as the economic powerhouses of the future.[107] India, Russia and Brazil share a light regulatory

[106] BRIC is the abbreviation used to describe the newly industrialised countries of Brazil, Russia, India and China.

[107] National Intelligence Council, (November 2008), Global Trends 2025: A Transformed World, (Washington, DC), highlights the importance of the BRICs.

regime, an acceptable IT infrastructure and a relatively weak state. China shares some of these attributes but is also suspected of sponsoring not just tolerating cybercrime.

In addition, other, smaller and different groups prosper elsewhere. At least until recently, Sri Lankan Tamil organised crime in the UK has been low key, even subcontracting operations to Malaysia and Singapore to avoid developing a local profile.[108] But it is also extremely competent, especially in the area of credit card fraud.[109] The drug cartels in Asia and Latin America are much more traditional in terms of organisation and focus but they are still massive operations in their own right and new groups are constantly entering the field.

However, the onset of cybercrime would appear to have blurred the distinctions between organised and opportunistic crime. In the BRIC countries and beyond, individual entrepreneurial IT-gifted individuals have also moved into this lucrative domain without apparently troubling organised crime groups. Traditionally, organised crime groups have maintained a forceful monopoly over their assets and their terrain, insofar as they dominated scarce and illegal commodities that would retail on the black market for inflated sums. But in the world of cybercrime, there appears to be little need for such a tight control over illegal markets. Whereas, at one time, oligopolistic or monopoly control over scarce or illegal resources was a key factor in generating massive profit margins, cybercriminals appear to see little reason to compete, protect and control as they have traditionally done in cities across the world.

[108] Interview with UK Home Office official, London, 26th June 2008.

[109] Sri Lankan Tamil organised crime groups have long been associated with credit card fraud, especially in and around West London petrol stations. Whereas they used to concentrate upon credit card 'skimming' and counterfeit chip and pin boards, they now simply sit in cars parked close to the petrol station and Bluetooth the financial data that leaves the tills. The information is then sent to a number of 'mules' who upload the information onto blank cards and use the cards immediately and for a limited amount of time. By the time the fraud centre is alerted, the card has been discarded.

2 Digital ecosystem

Innovation studies help us to understand the emerging digital business ecosystem. The diffusion of information and communication technologies has facilitated the growth of the environment in which cybercriminals operate.

Changes in the costs of research and development, production and skills, coupled with rapid technological changes, have been the main drivers behind the globalisation of company activities. Globalisation in turn has affected their organisation, which can be seen in the decentralisation of production and innovation activities and the greater collaboration with external partners. This has led to the growth of business networks, which are now ubiquitous throughout the economy.[110]

The business network has been compared to a biological system because the network is an 'organism' which responds to its environment and thus continually evolves.[111, 112] For instance, consumer tastes change through time and thus the constituents of the business network that supplies this particular consumer demand have to react accordingly to survive or do well.

A business ecosystem is "a loose network of suppliers, distributors and outsourced firms that work cooperatively and competitively to support new products, satisfy consumer needs and incorporate innovation".[113] These entities have different interests but are

[110] Corallo, A., Passiante, G., and Prencipe, A., (2007), *The Digital Business Ecosystem*. Cheltenham: Edward Elgar (Eds).

[111] Rothschild, M. (1990), *The Inevitability of Capitalism*. Henry Holt: New York, as cited in A. Corallo, G. Passiante, and A. Prencipe, A. (Eds.). (2007). *The Digital Business Ecosystem*. Cheltenham: Edward Elgar, p.1.

[112] Since the 1990s, scholars in innovation studies have increasingly described the business network in terms of a business ecosystem. See, for example, A. Corallo, A., G. Passiante, A. Prencipe, (2007), *The Digital Business Ecosystem* (Eds). Cheltenham: Edward Elgar; Iansiti, M., and Levien, R, (2004), "Strategy as ecology". *Harvard Business Review*, pp68-78; Moore, J. F., (1993), "Predators and prey: a new ecology of competition." *Harvard Business Review* (May-June), pp75-86; M. Rothschild, (1990), The Inevitability of Capitalism, Henry Holt, New York, as cited in A. Corallo, A., G. Passiante, A. Prencipe, (2007), *The Digital Business Ecosystem* (Eds). Cheltenham: Edward Elgar.

[113] Corallo, A., Passiante, G., and Prencipe, A., (2007), *The Digital Business Ecosystem* (Eds). Cheltenham: Edward Elgar.

interconnected with each other for their mutual survival and effectiveness.[114] Innovation is central to the creation, development and life of a business ecosystem and is a "catalysing element for the evolution of the ecosystem."[115]

Cybercriminals are increasingly operating in a business ecosystem in much the same way that companies such as Microsoft, IBM, Cisco and Hewlett Packard have successfully used the business ecosystem to define and establish their alliances and networks to sell their products and services. In particular, the traditional, ethnocentric organisational structures of criminal organisations have increasingly eroded to allow new sets of actors to make common cause, through networking and sub-contracting for example. As with companies, the cybercriminal ecosystem has done so by acquiring new partners, knowledge, ideas and skills to fuel innovation and thereby to expand the range of its cybercrime activities.

In a business ecosystem, the 'collective health' of other actors who influence the creation and delivery of the product or service is fundamental to a company's success.[116] In other words, there has to be innovation for a business ecosystem to thrive. "They [businesses] operate in a business environment of shared fates and business models, and see their ecosystems as helping them become more resilient to market changes… to achieve market success and sustain performance."[117] Similarly, the success of cyber-criminal activities require innovation to which individual criminals may not have be capable of undertaking productively. For instance, cybercriminals have continually to develop or acquire more sophisticated malicious software, if they are to infect more computer networks and become more effective and astute in stealing data and perpetrating credit card fraud. Moreover, they must remain adept at overcoming the preventative obstacles and the risk of identification and detection.

[114] M. Iansiti, and R Levien, (2004), "Strategy as ecology". *Harvard Business Review*, pp 68-78.

[115] J.F. Moore, (1996), *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystem*. Harper Business, New York, as cited in A. Corallo, A., G. Passiante, A. Prencipe, (2007), *The Digital Business Ecosystem*. Cheltenham: (Eds) Edward Elgar.

[116] M. Iansiti, and R Levien, (2004), "Strategy as ecology". *Harvard Business Review*, pp68-78.

[117] M. Iansiti, (2005), "Managing the Ecosystem." *Optimize Magazine* 4, www.optimizemag.com/article/showArticle.jhtml?articleId=59300381.

A digital business ecosystem is one that is facilitated by the extensive use of digital technologies, without which firms will be disadvantaged in their business operations.[118] Thus, cybercriminals involved in credit card and identity theft operate in a digital business ecosystem.

In essence, innovation studies tell us that a healthy digital business ecosystem requires:

- a fluid value chain that supports innovative activity and responds to changing needs and environment
- the capabilities required to undertake innovation
- the business models that are adopted to make the most profitable use of the various sources of capabilities.

2.1 The cybercrime value chain

The concept of value chain is a useful tool to understand the sequence of activities required to perpetrate cybercrime and how they link to each other.

Value chain analysis describes how activities integrate in the production of goods and services. This is a relevant framework for understanding the phenomenon of cybercrime and its dynamics.

Organisations are increasingly operating in a global environment. Globalisation is now understood not only as a mere expansion of economic activities across boundaries but also – perhaps more importantly – as the *functional integration*[119] of internationally

[118] Scholars have defined the digital ecosystem as the enabling technology for a business ecosystem. Digital technologies support the distribution of technologies and the development of "evolutionary business models for organizations." See P. Dini and F. Nachira, (2007), "The paradigm of structural coupling in digital ecosystems, " in A. Corallo, A., G. Passiante, A. Prencipe, (2007), *The Digital Business Ecosystem* (Eds). Cheltenham: Edward Elgar, pp.33-52, at p.42.

[119] Functional integration defines the way corporations (particularly multinational companies) are able to function as a globally integrated unit. A clear example is represented by large firms in the automobile industry, which are characterised by global fragmentation of their production, establishing complete manufacturing and assembly plants in numerous individual countries.

dispersed activities.[120] Digital technologies connected by the Internet have accelerated the rate at which this integration is taking place[121] and have also changed how economic activities are organised. As a result, they have transformed the relationships between production, consumption and power.

Falling communication costs and wide access to the Internet have led to what has been called the "death of distance",[122] enabling new international organisations as well as easily linking existing ones in remote sites. The Internet portrayal as the "network of networks",[123] acquires particular relevance in the context of cyberspace, as the environment where cybercriminal activities mainly take place. Cybercriminals can now operate across continents and may communicate only in cyberspace, as an encounter with Brazilian cybercriminals illustrates.

"For a month or so, KG disappeared. Max and SuperGeek attempted to contact him over Microsoft Messenger or IRC but in vain. This is common in a culture that prizes anonymity above all else. Like most such online relationships, the friendship between the three cyber pals was fragmented and based upon a minimal, yet intense, intimacy. They did not know where each other lived; what their socio-economic backgrounds were; or what they looked like." [124]

The concept of value chain is simple but very effective in further helping to explain the innovation approach to studying cybercrime.[125] Value chains describe the sequence of activities that are required to make a product or service, from conception to delivery and disposal. This sequence of activities involves the combination of inputs from various

[120] Dicken P., (1998), Global Shift: Transforming the World Economy, Paul Chapman, London.; Gereffi (2002), "The evolution of value chains in the Internet era", in Goldstein, A. and O'Connor, D., (2002), "Electronic Commerce for Development", OECD.

[121] This phenomena has been referred to as the new "information economy", a society characterised by its capacity to generate knowledge through global networks of individuals and organisations. Wall, D., (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press, UK.

[122] Cairncross, F. (1997), The Death of Distance: How the Communications Revolution Will Change Our Lives, Harvard Business School Press.

[123] Licklider, J. and Taylor, R. (1990), quoted in Wall, (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press, UK.

[124] Glenny, M., (2008) McMafia: Crime Without Frontiers, Random House, p.305.

[125] Kaplinsky R., and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

actors, which are increasingly distributed globally. This idea recognises economic activities as global, and its central concern is to unpack the relationships between the actors involved in the range of activities that lead to producing a good or service.

While value chains were intended to describe production of legitimate activities,[126] the similarities between the dynamics of cybercrime and those of private business mean that value chains can be easily applicable to the cybercrime 'industry'. Moreover, value chain analysis allows us to grasp the big picture and give perspective to individual anecdotes and isolated data.

Value chain analysis is a powerful and useful tool for both analytical and policy purposes. First, it locates particular **actors** within the value chain and shows how they change position over time. Second, it maps the common **flow of activities** required for the production of good and services. Third, it identifies the **linkages** between the various activities in the chain. Fourth, it helps us to see who gains along the supply chain and identify the strong and weak links. In other words, it identifies who plays an important role in its success, or how it is **governed**. Finally, it highlights the importance of **upgrading** and improvement. This latter aspect is particularly useful for understanding how criminals are improving their attacks, as well as for law enforcement to identify the core competences of cybercriminals.

The main goal of value chain analysis is to provide useful advice to legitimate firms on how to improve their ability to compete in the global economy. However, it may also help (a) unfold the structure of the cybercrime industry, and (b) identify major relevant areas for prevention of cybercrime, priority of action and alternatives for intervention.

[126] Much of the original thinking on value chains came from Porter M (1990), "Competitive Advantage" Free Press, London. However, the approach adopted in this report owes more to Kaplinsky R., and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa and to H Schmitz (2005), Value Chain Analysis for Policy Makers and Practitioners", ILO, Geneva. More recently the UK Department for Business Enterprise & Regulatory Reform has employed the concept of Global Value Chains in their analysis of the electronics and automotive sectors in Berr (2009) 'Globalisation of value chains and industrial transformation n the UK', February.

2.1.1 Mapping the cybercrime value chain

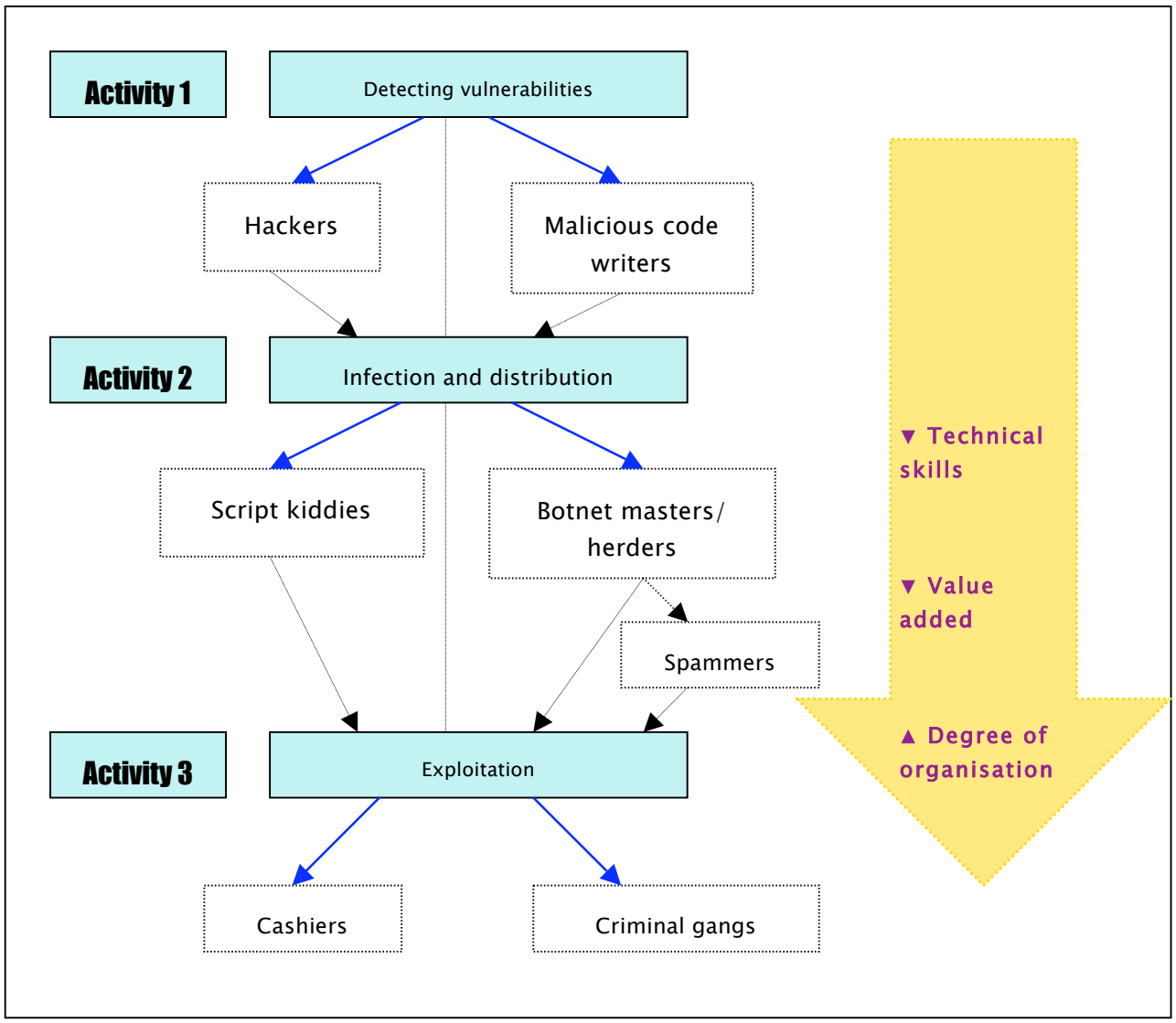
Most cybercrime attacks of credit card and identity fraud share the need to go through three basic activities: detecting vulnerabilities, infection and distribution, and exploitation.

Cybercrime has moved away from the fragmented activities of a few isolated programmers and is increasingly mimicking corporate business. The fraudsters seem to have defined roles and specialities and a clear division of labour. This applies to everything from ATM skimming to phishing and hacking. The actors involved in these crimes have specific means of communications, rules of engagement and even ethics. They coordinate their actions to gain competitive advantage – over the system they are attacking rather than from rival groups, given that the gains are so plentiful – and target a specific segment of the market.

Each of these activities is intended to support the undetected generation of financial profit. Therefore, each activity can be associated with multiple methods of achieving a financial reward (or business models as explained below), with their own sources of competitive advantage and associated gains or value added, combining with each other to form a value chain. Cybercrime can thus be seen as a whole value chain facilitating fraud, with different operations, profit margins, technological capabilities and innovation opportunities attached to each stage.

Cybercrime attacks resulting in identity theft and credit card fraud generally share the need to go through three basic activities. Various actors can perform these actions, either collectively or individually. The increasing trend towards specialisation is rapidly differentiating the tasks, which has improved the efficiency of each activity and subsequently the efficiency of the whole industry. The cybercrime value chain is represented in figure 8.

Figure 8: The cybercrime value chain



2.1.1.1 Detecting vulnerabilities

The **first activity**[127] consists of detecting vulnerabilities. The detection of security vulnerabilities requires a certain level of technical knowledge and skills and is the main occupation of hackers and malicious code writers.

Hackers are specialists in gaining unauthorised access to other computers.[128] Hacking is generally achieved through the application of particular tools, programming skills and computer knowledge, although it can be as simple as accessing password protected information.

Malicious code writers evolved from virus writers, but are mostly driven by economic profit rather than reputation, which will define the shift from the white-hat hacker motivated by the advance of knowledge to the cracker whose motivation is criminal. [129] Almost all crimeware programs have been written with a financial motive in mind. They can create zombies (hijacked computers) to launch denial-of-service attacks, phishing and spam mails. They can also create click and keystroke frauds, and steal application serial numbers, login IDs, and financial information such as credit card numbers and bank account information.[130]

It is important to note that in certain cases legitimate software tools have been adapted for crimeware purposes – user innovation will enable the move from legal to illegal boundaries. Some of the tools frequently used by hackers were designed for legitimate purposes, such as network administration or security auditing. For instance, the most widely used freeware hacking tool is Nmap, sophisticated port scanning software that can detect the services operating in a system, IP addresses and operating systems. This

[127] Despite its sequential representation, it is important to note that cybercrime is not a linear activity. While the three activities can be modelled as linear for ease of understanding, the functions are, more often than not, going on in parallel by different actors in the value chain, often in different parts of the world.

[128] Note the difference between black-hat hackers and white-hat hackers (see glossary). In this report we will refer to black hat hackers – this is, malicious hackers – as 'hackers' or 'crackers' interchangeably, since it is focused on criminal online activities.

[129] See glossary. The advent of PayPal is thought to have been an important factor in facilitating the move from competitive hacking to more remunerative activities.

[130] Shih-Yao Dai Sy-Yen Kuo, (2008), MAPMon: A Host-Based Malware Detection Tool, 13th IEEE International Symposium on Pacific Rim Dependable Computing.

tool is used by security and networks administrators to manage their systems, as well as by hackers to exploit vulnerabilities. Security firms (gamekeepers) often hire reformed crackers to write their security programmes.

Other software, however, is undoubtedly malicious as well as invasive, combining the motivations and skills of both the cybercriminal and the white-hat hacker. For instance, MPack has become one of the most popular software exploitation tools in the underground markets. Mpack is malware kit produced by Russian crackers in 2006 that not only finds vulnerabilities but also exploits them by automatically storing relevant data for its later use. Our interviews with IT specialists suggested that there is there is a fine line between legitimate software and crimeware, since it is its *use* that generally turns it into a criminal activity.[131]

'Dual-use' technology

Recent research identified a criminal gang using software tools normally reserved for computer network administrators to infect thousands of PCs in corporate and government networks with programmes that steal passwords and other information. Security experts say that although attacks against network administrators are not new, the systematic use of administrative software to spread malware had not previously been widespread.

The gang was identified publicly in May 2008. SecureWorks, a computer security firm in Atlanta, determined that the Russian-based gang was able to put in place a central programme controlling as many as 100,000 infected computers across the Internet. The program was running at a commercial Internet hosting computer centre in Wisconsin. After law enforcement agencies were alerted, the original command programme was shut down. However, the gang immediately reconstituted the system, moving the control programme to another computer in the Ukraine, beyond the reach of law enforcement in the United States.

Source: John Markoff, (2008), "Russian Gang Hijacking PCs in Vast Scheme", *The New York Times*, 6 August 2008.

[131] Interview with Brian Moore, IT specialist, 17th November 2008.

Traditionally, hackers have been depicted as individuals who work in isolation but in competition with each other, and who are passionate about their particular area of malicious interest and prepared to devote enormous time and energy to developing their ideas and implementing them. Hackers often share their ideas in user communities and many such communities are characterised by an open sharing of ideas and innovations, termed 'free revealing'.[132] Innovative users are often seen as a significant agent of technological change although such change may not always be welcomed by society.

For example, hackers may well be the leading edge of a market trend and conform to the notion of lead users.[133] However, in other cases they may act more like a subversive group whose aim is to break technical and legal boundaries. Coupled with the magnifying effect of the Internet their influence will be increased by free revealing, enabling a relatively small number of technically able individuals to have an impact on society that is disproportionate to their numbers or social and professional positions. However, new evidence suggests that hackers and malware writers are moving away from working individually or in groups with common goals, to gradually enter the hierarchical structure of cybercrime organisations, where they have their own well-defined role and reward system.[134] This is further explored in the sections below.

It is also likely that there are relatively few attackers, exploit and malicious code developers. Due to the technical nature of these skills, fewer individuals are adept at conducting attacks, doing security research, or developing exploit code and attack tools.[135]

2.1.1.2 Infection and distribution

The **second activity** involves the distribution of detected vulnerabilities (such as malware) and the subsequent infection of computer systems. Hackers and malware

[132] Harhoff, D., Henkel, J., & von Hippel, E. (2003). Profiting from voluntary information spillovers: how users benefit by freely revealing their innovations. Research Policy. 32 (10), 1753-1769.

[133] Von Hippel, E., 1986. Lead Users: A Source of Novel Product Concepts, Management Science, 32 (7), July, pp791-805.

[134] Finjan Malicious Code Research Centre, (2008). Web Security Trends Report Q2 2008. See www.globalsecuritymag.com/Finjan-Discovers-Compromised, 20080506, 2911.

[135] Symantec, (2008), "Symantec Report on the Underground Economy", July 07–June 08.

writers do not necessarily know how to exploit the vulnerabilities they identify; in other cases they are simply not willing to cross the safe line of legality.[136] Therefore, they need to distribute and sell their products to the next agents in the value chain. The products from hackers and malware writers are generally used by script kiddies (unskilled hackers) and botnet owners/botnet herders (those who run collections of compromised computers).

'Script kiddies' usually describes those who use scripts or programmes developed by others to attack computer systems and networks. They are named 'kiddies' as they are generally assumed to be juveniles lacking the ability to write sophisticated hacking programmes on their own. They often use hacking manuals, free malware or do-it-yourself virus kits to search for vulnerabilities and exploit security breaches. Their participation in organised networks or gangs is supposedly limited, so we will not focus on their activities here. However, they are still considered dangerous because of their irresponsible use of sophisticated software.

Much less is known about the dynamics of botnets. Bots are malware programmes that are installed silently without the consent of the user. A botnet is a network of computers on which a bot has been installed, and is usually managed remotely from a command & control (C&C) server. The main purpose of botnets is to use the computers they have hijacked (also named 'zombies') for fraudulent online activities. They can be created by an individual (a hacker or a malware writer) but are generally managed by a group of criminals or an organised crime syndicate.[137] Botnets can be exploited directly for identity theft or to spread mass campaigns of unsolicited e-mails (spamming) or scams. But evidence suggests that operators of botnets frequently sell their services to spammers, mailing out spam runs over thousands of infected computers that cannot be linked to the source.[138] These aspects are followed up below.

[136] Note that in the UK, as in many other countries, misappropriation of data or writing malicious software does not constitute a civil crime but only its exploitation.

[137] Barroso, D. (2007), ENISA Position Paper No. 3; Botnets – The Silent Threat.

[138] Terrence Berg, (2007): Cybercrime new internet threats create challenges to law enforcement, Computer Law Journal, June 2007.

Recent estimates state that about 3,000 different botnet command & control servers[139] are known to be operating every day, with each botnet averaging 20,000 compromised computers.[140]

2.1.1.3 Exploitation

The **third activity** involves the final exploitation of the stolen information obtained through the cyber attack: turning the traded data into cash. When criminals obtain the stolen data (personal information, credit card and bank details), they must use it to steal money. This is not without risk, and this is where the chance of detection and arrest increases significantly.[141]

This activity involves high risk and lower technical capabilities, and can be easily embraced by organised criminal gangs and individual agents looking for money.[142] There are many ways to exploit information obtained from illicit means. Some involve technical skills while others require no more than the ability to use an ATM.[143]

For instance, cloning credit cards requires a minimum understanding of technical procedures. Cybercriminals install a false front to ATM machines that conceals a device capable of cloning all the relevant card details necessary to create a digital copy. First, a scanner reads the magnetic stripe on the reverse of the card to capture the card data, which contains the 16 digit card number, the card start and expiry dates, the cardholder's name and the security number on the card. Second, a small digital camera photographs the card owner entering the PIN code, providing the owner does not

[139] Command & control infrastructure is the system that remotely sends instructions to the hijacked computers (zombies) that comprise the botnet. This is done via an IRC (Inter Relay Chat) server installed illegally. If the command-and-control is disabled, all the machines in the botnet become useless to the botmaster.

[140] Some C&C servers manage just a few infected computers (~10), large ones manage thousands of bots (~300.000) – Barroso, (2007), ENISA Position Paper No. 3; Botnets – The Silent Threat.

[141] Kaspersky, (2005), "The changing threat, from prankster to professionals".

[142] Russian crime groups, for example, minimize the risk of being caught by selling the credit card information to, amongst others, Nigerian groups who are more prepared to take the risk of being caught. In London, recently, a Latvian criminal was caught when a long queue of ATM users complained to the police who arrested the user in possession of a large number of credit/debit cards complete with pin codes written on each card. He was only detected because he was too lazy, incompetent or impatient to move from one machine to another. These users can net over £20,000 a week. Interview with Roy West, Cheque and Credit Card Unit, City of London Police, 9th December 2008.

[143] Details on the examples of this are provided in the following section on dynamic capabilities.

conceal this. Third, the device contains a memory stick, which records all this information for fraudsters to recover and start using these stolen cards.[144] There is a low level of technical knowledge necessary to operate the cloning kits. According to a fraud investigation director of a large bank, Romanian gangs seem to monopolise this activity.[145] The information is used to generate fake cards and withdraw money from ATMs or make purchases. To turn these cards into cash, criminal gangs generally develop a network of 'runners', who extract money from cash points for a commission.

Other forms of exploitation do not require any technical skills. Many buyers of stolen data also use the services of experienced individuals who will convert the stolen goods, such as bank account credentials, into online currency accounts or money transfers.[146] These people are called cashiers. Drop services provide criminals who have purchased items online with stolen credit cards with a convenient and reliable address to which they can mail stolen goods. In exchange for these services, cashiers and drop services charge a fee, which is usually a percentage of the cash involved in the transaction.[147]

2.1.2 Linkages between cybercriminals

Cybercriminals link mostly over Internet Relay Chats and illicit web forums, which serve as meeting points and marketplaces for fraudsters.

Value chain analysis also highlights the relevance of understanding dynamic linkages between the activities along the chain. Links between productive activities go beyond particular sectors and firms. By concentrating on the nature of the connection among all actors, value chain analysis allows us to uncover the flow of economic, organisational and coercive activities between producers within different sectors on a global scale.[148]

In the cybercrime value chain we could consider two types of link. First are those within each criminal organisation and between hackers and cybercriminal networks. There has

[144] 192.com Business Services, (2008), *The Fraudster's Modus Operandi*. London, p.8.

[145] Interview with the Director of a fraud investigation unit of a leading financial institution, 26th November 2008.

[146] Symantec, (2008), "Symantec Report on the Underground Economy", July 07–June 08.

[147] Jaikumar Vijayan, 20th October 2007, 'A Hacker's Holiday Shopping List, Computerworld.

[148] Kaplinsky R, and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

been much speculation and debate as to the level of organisation of these groups. Unfortunately much more is known about what they *can* do than about *who* is behind them, let alone details about how these actors link together.

The one thing we know is that in the cybercrime business most participants connect on the Internet. Web forums and Internet Relay Chats (IRCs)[149] are the marketplaces where buyers and sellers meet and exchange ideas, goods and services - and payment arrangements. The purpose of illicit forums is to allow cybercriminals to communicate anonymously and in real time.

A year-long research study on underground web forums and IRCs created and run by cybercriminals[150] identified three primary types of trader on underground economy servers: sellers who advertise their goods and services for sale; potential buyers; and requesters who post advertisements for specific items to buy.

Web forums and IRCs are operated by the administrators, and although they both serve the same purpose, there are fundamental differences between them. In web forums, potential vendors are subject to peer-reviewed processes before they are granted vendor status. Participants of web forums tend to be more established, and are generally accessed by invitation-only. Their strength as a solid link for cybercriminals is also their main weakness, since they are easier to trace.[151] In contrast, IRCs are mainly based on reputation and virtually anyone can advertise. As a consequence IRCs have more traffic and are becoming more popular marketplaces between fraudsters. However, their transitory nature makes it more prone to admit 'unethical' criminals or law enforcement agents. To overcome this weakness, one of the services offered in IRCs are 'checking' services, to assess the validity of the data offered, such as card numbers and CVV2 numbers.

[149] Real-time Internet text messaging mainly designed for group communication in discussion forums.

[150] Symantec, (2008), "Symantec Report on the Underground Economy", July 07–June 08.

[151] Symantec, (2008), "Symantec Report on the Underground Economy", July 07–June 08.

Fraud on fraudster

The most recent step in the commoditisation of phishing is the distribution of *free* phishing kits. These kits are actively advertised and distributed in underground IRCs at no charge. Free phishing kits hide backdoors through which the phished information is sent to recipients (probably the original kits' authors) other than the intended ones (Cova et al, 2008).

An example is a recent phish kit targeting the Bank of America, reported at Netcraft in 2008, which contains an interesting insight into the intellectual hierarchy involved in Internet fraud. The phishing kit looks attractive to any fraudster – it is straightforward to deploy on any web server that supports PHP,[152] and a single configuration file makes it easy to specify an electronic mail address to receive captured financial details. In addition to requesting the credit card numbers and bank account details, a second form on the phishing site asks for the victim's SiteKey challenge questions and answers,[153] which can help a fraudster gain access to the victim's Internet banking facilities.

Sources: Marco Cova, Christopher Kruegel, and Giovanni Vigna: "There is No Free Phish: An Analysis of "Free" and Live Phishing Kits", 2008; and NETCRAFT news at http://news.netcraft.com/.

Recent research on underground forums has provided valuable information about the way cybercriminals form alliances, contact specialists in complementary techniques or find individuals who can extract cash for them.[154]

[152] PHP (PHP Hypertext Preprocessor) is an open-source scripting language used to create dynamic web pages, PHP can also be used to connect to a database; to retrieve, add or update content.

[153] SiteKey questions and answers is a method of authentication to prevent unauthorised access to a person's account. The questions are only shared between the financial institution and the customer. Their primary purpose is to deter phising.

[154] Symantec (2008), "Symantec Report on the Underground Economy", July 2007–June 2008; Finjan (2008), Malicious Code Research Center, Web Security Trends Report Q2 2008.

2.1.3 Governance

Value chain analysis highlights the need to understand the distribution of power along the chain. The cybercrime value chain is coordinated via the Internet by both buyers and producers of crimeware.

Another central contribution from value chain analysis is the importance it places in characterising the power asymmetries in global value chains. In value chain analysis governance is defined as the power to determine who participates in the value chain, what is produced, how and when, and asymmetries (imbalances) in market power. What matters most is who determines the overall character of the chain and who governs it? The concept of governance is crucial in for three main reasons. First, leading actors in the chains can have a major impact in creating and shaping new markets. Second, they can help determine the price, quality and speed of production. Third, they can help determine the distribution of gains and profits along the chain.

Building on this concept of governance, a broad distinction can be made between three types of value chain. The first describes the value chain where buyers set the rules, namely, *buyer-driven chains*. Buyer-driven chains generally describe those industries in which the specifications of the products are supplied by the large retailers or marketers that order the goods. The second describes industries where key producers, generally commanding vital technologies, coordinate the various links – *producer-driven chains*. This latter is characteristic of capital and technology-intensive industries.[155]

These two basic categories automatically expand if we consider that, first, some value chains exhibit very little governance and, second, some chains may embody both producer- and buyer-driven governance.

Given these limitations a third type of value chain has been defined, namely, the *Internet-oriented chains*, representing the dynamics of firms operating in the expanding digital economy and e-commerce. This distinct chain is composed of the firms that make Internet transactions possible, from computer manufacturers to Internet service providers. These chains are characterised by the virtual integration of their participants

[155] Kaplinsky R, and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

and facilitated by an explosion in connectivity due to the open and almost cost-free exchange of information.[156]

In technology-intensive industries, it has been suggested that the ability to govern often rests in intangible competences (such as R&D and design) into which it is difficult for other firms to break.[157] Inherent to cybercrime is the constant search of new technologies for exploitation; however, this requires substantial investment in R&D, training and human resources, which is where traditional organised crime may have a significant role as investors.

Organised criminal groups are gradually diversifying from traditional criminal activities to more lucrative and less risky e-crimes by co-opting a diverse array of technically competent cybercriminals. Although traditional criminal organisations generally lack the technical skills to generate crimeware, they have vast funds from traditional criminal activities to recruit highly skilled individuals and pay for their services, even sponsoring university degrees.

Organised crime syndicates are in a position to fund computer science courses at university in return for cybercrime expertise after the course has finished. The chief information security officer for a large multinational recently said: "[cybercrime rings] have research and development programmes, they are putting people through university,[158] they are calculating return on investment and they have better quality assurance. By comparison, the legitimate security industry is under-funded, under-resourced and constantly on the back foot."[159]

The preliminary findings for this overview indicate that we can find examples of each of these value chains for various segments of the cybercrime 'industry'. In certain criminal

[156] Gereffi, G., (2001): "Beyond the Producer-driven/Buyer-driven Dichotomy. The Evolution of Global Value Chains in the Internet Era", IDS Bulletin Vol 32 No 3 2001.

[157] Kaplinsky R, and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

[158] Interview with a Tamil who had been charged with credit card fraud.

[159] Paul Simmonds of AstraZeneca, quoted in Marshall Kirkpatrick, (23rd June 2008): Students: The New Hiring Frontier Online, for Good and Evil. See: http://www.readwriteweb.com/archives/students_the_new_hiring_frontier.php.

activities, such as credit card cloning and spamming, we can detect features of a buyer-driven value chain since organised crime appears to have a major role in setting up the prices and leading the direction of new markets. Customer demand, in this case, emerges as a key driver of change in the value chain. In other segments, such as botnet management and hacking, we can detect features of a producer-driven value chain, since malware writers and hackers tend to establish the prices and rules of the market. Overall, the Internet-oriented chains best represent the complex, non-hierarchical and virtual integration of activities in which cybercrime is rapidly evolving. However, given the role of traditional organised crime groups, which become involved at the development phase but maintain as well their traditional activities (e.g. trafficking, racketeering, slaving)[160] there may be scope to develop a fourth cybercrime-specific value chain.

2.1.4 Upgrading

The speed of upgrading in the cybercrime world is so fast and dynamic that the most competitive gangs gradually combine process, product, functional and chain upgrading.

The capability to innovate is vital to the continuous improvement of products and processes. However, value chain analysis stresses that innovation needs to be consider against that of competitors. This process of innovation, in an industry formed by many global actors competing and integrating with each other, is what is understood as upgrading.[161]

Value chain analysis identifies four trajectories which firms can adopt in pursuing the objective of upgrading, namely process, product, functional and chain upgrading. Some examples of these types of upgrading are featured through the case of the Storm Worm botnet below.

[160] This was, in part, to secure the flow of funds but also to preserve market presence and activity in another commercial environment.

[161] Kaplinsky R, and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

The Storm botnet case study: the survival of the fastest in upgrading

The Storm Worm botnet is a global network of compromised computers that was estimated to control between one and five million machines, and is capable of sending over three billion spams a day. Initially, the Storm Worm gang relied on social-engineering techniques to lure victims to open an attachment that contained a piece of malicious malware, a Trojan. This Trojan silently took control of the infected machines and linked them together into a botnet, which was mainly used to send vast amounts of spam and distributed denial of service attacks (DDoS). For some months, Storm Worm was simply spreading and gaining strength, rapidly becoming one of the largest in the world. It even started developing upgraded malware to avoid signature-based detection, with new variants being created every 15 minutes.

Soon the Storm Worm had become the base that nearly all cybercriminals use to exploit the Internet and hide their theft of millions of users' identities. By the end of 2007 it was reported to comprise around 13 per cent of the entire malcode set collected. In 2008 Storm Worm launched for the first time a large blended attack that combined sophisticated social engineering with malware [*product upgrading*] that not only enrolled the infected PCs as part of Storm's botnet but also captured keystrokes, load viruses, copy and transmit or delete files [*functional upgrading*].[162]

To remain operative, the Storm Worm botnet controllers introduced innovative improvements in their camouflaging techniques. Currently, the locations of the remote servers that control the botnet are hidden behind a constantly changing Domain Name System (DNS) using a technique called 'fast flux'. This technique changes the name and location of the DNS servers, often on a minute by minute basis, making external monitoring and disabling of the system more difficult. There is no central 'command and control point' in the Storm botnet that can be shut down [*process upgrading*].

To add to these developments, there has been a recent segmentation of the botnet into smaller, more discreet networks, which allows the controllers to hire-out each segment

[162] Vikram Thakur from Symantec noted how Storm Worm moved from simply using social-engineering techniques to spread malware to actually exploiting vulnerabilities.

to different groups of criminals for different purposes. The rapid evolution of the Storm Worm gang has turned into an Internet Service Providers (ISP) for cybercriminals [*chain upgrading*].[163]

Sources: Ian Grant (14th Feb 2008): Storm Worm is basis for most cyber attacks, Computer weekly.com/ Bruce Schneier (10th April 2007): Gathering 'Storm' Superworm Poses Grave Threat to PC Nets, Wired.com/ Sorensen, Chris (15th October 2007). "Storm Worm the 'syphilis' of computers", The Star. Retrieved on 17 October 2007. / Symantec (2008) Evolved Storm Worm attack brewing/ Pedro Hernandez (5th April 2008) MessageLabs: Storm Botnet Spews 20 Percent of All Spam, eSecurityplanet.com.

Process upgrading. This type of upgrading manifests itself in increases in the efficiency of internal processes such that these are significantly better than those of rivals. Process upgrading can take place within individual links in the chain and between the links in the chain.[164] The cybercrime industry is replete with examples including the dynamics of botnets. The two main goals of a botnet can be summarised as infecting as many users as possible through the use of new propagation techniques and increasing stealth. These two factors drive process upgrading in cybercrime in general but are particularly applicable to botnets. In the Storm botnet (see box), attackers have become more cautious and sophisticated in their process of distribution and delivery, constantly upgrading their camouflage techniques to avoid detection, as reflected in the development of fast-flux.

Product upgrading. This refers to the ability to introduce new or improved products faster than rivals. This involves changing new product development processes both within individual links in the value chain and in the relationship between different chain links.[165] Highly sophisticated crimeware is constantly evolving in complexity and

[163] Paul Wood, a Senior Security Analyst for MessageLabs said in April 2008: "The way in which the Storm botnet has evolved from its dawn in 2007 has placed it head-and-shoulders above many other operators in this market. i.e. the market of creating and hiring-out botnet airtime to spammers and other online criminals," They have basically become an Internet Service Providers (ISP) for cybercriminals

[164] Kaplinsky R, and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

[165] Kaplinsky R, and Morris M., (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa.

accelerating on a monthly basis. With Storm Worm, we can see the agility of cybercriminals in releasing upgraded versions of malware and blended attacks. In other cases, malware acquires improved functions compared with its rivals and even substitutes itself for malware installed by competitors. Unlike hackers, such groups do not appear to compete with each other or protect against other types of groups where there would seem to be little rivalry given the abundance of 'booty' available. Consequently, there is no need to compete over resources since they are far from scarce. The rivals here are the law enforcement agents who seek to identify and shut down their operations.

Another recent example of product upgrading can be seen in the Conflicker worm which emerged in late 2008 and sought to integrate millions of inflected computers to create a giant botnet. Computer experts worry that it could become a profitable platform for massive Internet fraud and theft. They also increasingly suspect that Conflicker will hold computers to ransom. According to IT experts, Conflicker's software developer(s) has repeatedly updated its software in a cat and mouse game. Researchers who have been painstakingly disassembling the Conflicker code have found difficulty in determining where the author(s) is located, or the organisation underlying the development of the worm, or whether the programme is being maintained by one person or a group of hackers.[166]

Functional upgrading. This refers to increasing value added by changing the mix of activities conducted within the firm. This implies either integrating activities that were not performed in the firm before or outsourcing them (an example in a legitimate business would be outsourcing or taking responsibility for accounting or logistics).[167] There are multiple examples of functional upgrading in the cybercrime business, where evidence suggests that certain gangs have expanded their core activities. In the Storm Worm example, functional upgrading is illustrated by their move from simply spreading malware to the actual exploitation of vulnerabilities. Tamil cybercriminals in London are thought to have subcontracted parts of their operation to South East Asia to enable them to maintain a low profile on the streets and avoid the adverse attention of other gangs.

[166] John Markoff, "Computer experts united to hunt worm", New York Times, 18th March 2009.

[167] Kaplinsky R, and Morris M., (2001).

Chain upgrading. This refers to the moving to a new value chain.[168] In a legitimate business this could involve a move from manufacturing radios to computers. In Storm Worm upgrading is exemplified by their move from spamming to becoming Internet Service Providers for criminals.

2.2 Capabilities and specialisation

Specialisation is causing changes in the skills needed to perpetrate cybercrime at different points in the value chain. Cybercriminals adapt their capabilities to create and exploit opportunities for innovative forms of credit card fraud and identity theft.

The second component of the ecosystem relates to capabilities. A firm's capability is "a collection of routines that confers upon an organisation's management the ability to produce significant outputs of a particular type".[169] Scholars, however, argue that dynamic capabilities, more than just 'routine' capabilities, are required to create and sustain competitive advantage in a changing business environment.[170] Dynamism connotes change, so dynamic capabilities are those that extend, modify or create ordinary capabilities[171] to meet the challenges and demands of the marketplace. Such capabilities therefore underpin the ability of an organisation to make best use of new equipment or technologies to produce novel and innovative products or services, and hence improve their productivity and competitive advantage.[172] Dynamic capabilities may be developed from within the firm through training[173] or through continuous

[168] Kaplinsky R, and Morris M., (2001).

[169] Winter, S. G., (2000), "The satisficing principle in capability learning." *Strategic Management Journal* 21 (Oct-Nov (special issue)): pp.981-996.

[170] Teece, D., G. Pisano, and A. Shuen, (1997), "Dynamic capabilities and strategic management." *Strategic Management Journal* 18: 509-533.

[171] Winter, S.G. 2000. (Winter. S.G. (2002). Understanding Dynamic Capabilities, http://bus8020kelly.alliant.wikispaces.net/file/view/Understanding+Dynamic+Capabilities.pdf.

[172] Bessant, J., and S. Caffyn, (1997), "High-involvement innovation through continuous improvement." *International Journal of Technology Management,* 14(1), 7–28; Rao, S., Tang, J., and Wang, W., (2002), "The Importance of Skills and Innovation and Productivity." *International Productivity Monitor*, 4, 1-26.

[173] Bessant, J., and J. Buckingham, (1993), "Organizational learning for effective use of CAPM." *British Journal of Management,* 4(4), 219-234.

improvement and the introduction of new processes.[174] As with firms that deploy home-grown capabilities to create competitive advantage or a market niche, cybercriminals appear also to have some in-house capabilities to carry out their activities and easy access to buy in the required capabilities. This may reflect the complete absence of norms or legislation preventing such change and the eclectic mix of actors involved.

Value chain analysis understands specialisation in a context of 'systemic competitiveness', where individual firms operate in a wider system of suppliers, customers and competitors. This may be located locally, regionally or internationally. Within this 'ecosystem', the identification of the firm's distinctive competencies leads the process of specialisation and determines the behaviour of the individual firm within the value chain.[175]

This is all relevant to cybercrime. The roots of modern cybercrime capability lie in the work of individual hackers who sought infamy through the disruption of as many PCs as possible, the benchmark by which they would be judged by peers. The cybercrime ecosystem has since become the playing field for criminal organisations and organised criminals who have realised the potential for fraud on the Internet and have made common cause with hackers reconfiguring their capabilities for their own profit.

Specialisation often implies higher barriers of entry; the higher the barriers, the greater the profitability. Technical skills, organisational capabilities and levels of risk all limit those who have the requisite skills, though some of these barriers are introduced by law enforcement agencies, security firms and software companies.

At the top of the chain are 'harvesting fraudsters' (hackers, malware writers and botnet owners). At this level we find evidence that criminals are becoming more advanced and sophisticated in the techniques to gather exploitable data.[176] Higher technical capabilities

[174] Bessant, J. and Caffyn, S. (1997), "High-involvement innovation through continuous improvement." *International Journal of Technology Management,* 14(1).

[175] Kaplinsky R, and M. Morris, (2001), A Handbook for Value Chain Research. International Development Research Centre: Ottawa. p.9.

[176] Interviews conducted with IT specialists suggested that the IT skills required by various cybercrime activities range from those expected of 2nd year undergraduates up to post-graduate qualifications (interviews with Professor Richard Clayton on the 21st November 2008, and Brian Moore in London 17th November 2008).

allow them to secure high profit margins and maintain the barriers of entry. Meanwhile, at the lower level of the chain, criminal activity (the cashiers and criminal gangs) is becoming more sophisticated in organisational management, increasing the number of victims and multiplying their comparably lower profit-margin activities.

2.2.1 Capabilities and specialisation for data harvesting

(a) Use of non-cyber skills to harvest data.

Credit card fraudsters and identity thieves use a combination of 'traditional' skills to acquire data and perpetrate fraud. Rummaging in trashcans for personal and financial data is a tried and tested way but increasingly unrewarding as more people now use shredders. Rummaging is also time consuming and can sometimes yield little for the effort expended whilst running the risk of being caught or arousing suspicion.[177]

A quicker, more effective and increasingly common method involves working with 'subcontractors' or thieves. Cybercriminals pay them well - each card is worth £250 and if accompanied by a PIN, it fetches about £500.[178] 'Insider agents', employees of companies such as in financial institutions, call centres and bars and restaurants are the prime targets. "They [the fraudsters] just brazenly hang around outside the office complex gates," admits a Risk and Security Manager of a leading online computer retailer.[179] Prices will be lower if the call centres are in low cost countries, such as India, where passwords, addresses and passport details can change hands for a little more than £4.[180]

Credit card fraudsters and identity thieves directly approach potential accomplices who have two distinct characteristics: (1) those who have easy access to customers' personal or financial details; (2) those in poorly paid jobs with access to financial data, so the financial incentive is so attractive that it outweighs concerns about collusion with the fraudster. Fraudsters who use this approach report a high level of cooperation and admit

[177] According to a manager in a credit checking company the "going rate" for three 'identifiers' for the same individuals was worth £5 to the homeless in Camden who were 'contracted' to rummage through the rubbish bins. Identifiers which could be used to apply for a passport was worth £50. Interview conducted on 29th January 2008.

[178] 192.com Business Services, (2008), *The Fraudster's Modus Operandi*. London.

[179] 192.com Business Services, (2008), *The Fraudster's Modus Operandi*. London.

[180] Biswas, S., (2005) How secure are India's call centres?, BBC News, 24 June, http://news.bbc.co.uk/2/hi/south_asia/4619859.stm.

that employees are more concerned about getting caught by their employer than about the law or morality of their conduct.[181]

Our interviews with directors of fraud investigation units in leading financial institutions confirm this view. However, they point out that in an economic environment in which job stability is elusive threatens, loyalty to the employer. Hence there is always the temptation of quick financial rewards. Thus employees are now increasingly less worried about the employer too. One interviewee suggested that the 'instant gratification' of today's culture contributes to the readiness of employees to compromise confidential data. And such behaviour is not limited to those in low paid jobs.[182]

Another way illegally to obtain data is by mail interception. Fraudsters have a variety of strategies for accessing post once it is delivered. These include targeting properties with external or multiple mailboxes in a secure area, or by gaining access to the property itself. More sophisticated fraudsters will have a range of safe addresses and will arrange for particular items of mail to be redirected, perhaps by advising the bank of a change of address, ordering a duplicate card, or reporting a lost card and requesting a new card and pin number.[183,184]

(b) Use of cyber capabilities to harvest data.

Credit card fraudsters are becoming much more adept at exploiting new technologies for their criminal activities. They are keeping pace with technological developments and even outpacing them through the adaptation and upgrading of existing software tools.

[181] 192.com Business Services, (2008), *The Fraudster's Modus Operandi*. London.

[182] These directors also highlight a greater concern with insider agents than external fraudsters. One director of the fraud investigation unit of a leading financial institution also noted that debit card fraud is more significant than credit card fraud. This is because debit card transactions are processed the same day, whether they are domestic or international. So this makes it easier for "insider" debit card fraudsters to operate. Interview conducted 26th November 2008.

[183] Interviews with directors of fraud investigation units of two leading financial institutions, 11th and 26th November 2008. For details on how mail interception is carried out, see 192.com Business Services, (2008), *The Fraudster's Modus Operandi*. London.

[184] According to Experian (2008) redirecting a person's post to a different address, continues to grow in the UK as means of perpetrating ID theft. Experian (May 2008): Victims of Fraud Dossier.

At the higher end of the *generation* of crimeware tools and distribution (harvesting fraudsters), increasing specialisation poses greater challenges for the prevention of cybercrime. IT security companies and law enforcement agencies often highlight the difficulties involved in preventing the next threat. An IT expert summarised it in thus: "One of the problems with forecasting is that companies and individuals need to protect themselves against a wide spectrum of threats. However, skilled cybercriminals can focus on one single threat and distil it, take it to perfection. This allows them to be always ahead of protection techniques."[185]

Another IT specialist said: "There are new tactics each month and next year there will be something we haven't even thought of yet. It is difficult to create a model of the threat when we don't know what is going to happen."[186] Security and technology providers currently devote substantial time and money to detecting and preventing such crimes, but it is difficult to second guess and anticipate every innovation. The Conflicker worm shows the dynamic capabilities of cybercriminals. Several people who have analysed various versions of the programme have suggested that the Conflicker author was monitoring efforts by computer experts to tackle the potentially widespread infection that the worm might create. Conflicker has already been through several versions and the current version (Conflicker C) involves a major rewrite of the software allowing it to disable many commercial antivirus programs as well as operating systems' update features.[187]

An interview with an IT security company stressed that there needs to be a shift in the way we perceive IT security, since reactive technologies such as detection by reputation,

[185] Interview with IT specialist Brian Moore, London 17th November 2008.

[186] Brian Scheler as quoted in Jane Wakefield, "Thieves set up data supermarkets", BBC News, 23rd April 2008; available at: http://news.bbc.co.uk/1/hi/technology/7363422.stm. We have only to find two pieces of work which attempt significant forwards looks in the field of cybercrime. These include the Foresight programme report of the Cyber Trust and Crime Prevention project entitled "Gaining Insight from Three Different Futures" (2004), Office of Science and Technology and a reference to reports produced by the Future Scanning Sub-Group of the Police Science and Technology Group (whose website is no longer accessible) referred to in P. Ekblom "How to police the future: scanning for scientific and technological innovations which generate potential threats and opportunities in crime, policing and crime reduction" in J. Smith and N Tilley Eds. (2005) "Crime Science: New approaches to preventing and detecting crime", William Publishing, Devon.

[187] John Markoff," Computer experts unite to hunt worm" New York Times, 18th March 2009.

origin or signature or a presence on a blacklist,[188] is not enough to keep pace with the diversification and complexity of advanced web techniques being used by the criminals.[189]

Technological cat and mouse game

The dynamics between the crimeware producers and the IT Security companies have been often described as a constant game of cat and mouse, since cybercriminals do not stand still when one of their avenues for distribution is closed. These dynamics were well represented by an example given by one of our interviewees, from an IT security company. One of the company's services is managing their customers' spam. But they face the increasing sophistication of spammers.

Initially spammers used to disguise words with spelling mistakes to overcome the filters. When the IT experts realised this and devised ways to counter it, the spammers started sending messages embedded in a graphic instead of plain text, since they are harder to scan for spam filters. When this was detected and dealt with, spammers rapidly started using animation graphics to confuse the filters. They always seemed to be several steps ahead of the IT experts in security firms.

Source: Interview Simon Heron, London 10th November 2008.

Criminals are also cleverly exploiting vulnerabilities in websites to plant malicious code in newly-discovered browser exploits[190] to infect the computers, crash the network or computers, and to solicit and steal data. According to a survey conducted by a large multinational IT company 94 per cent of all browser exploits in 2008 occurred within 24

[188] Blacklist detection is based on the detection of viruses through a black list constructed on the basis of malicious code threats that have been identified in the past. However, this method has been largely criticized by its limitation to keep pace with the volume and variations of malware released every hour.

[189] Interview with Tim Warner, Finjan, 17th November 2008.

[190] A browser exploit is a piece of code that exploits a software bug (flaw, failure or fault) in a web browser such that the code makes the browser do something unexpected, including crash, read or write local files, plant a virus or install spyware. A web browser is a software application, which enables a user to display and interact with text, images, videos, music, games and other information typically located on a web page. Examples of web browsers are Google, Mozilla Firefox and Internet Explorer.

hours of an official vulnerability disclosure. The survey also revealed that in the first half of 2008 attacks targeting flaws in browser plug-ins are increasing markedly.[191] Also in the first half of 2008, around 78 per cent of web browser exploits targeted browser plug-in bugs.[192] Web browser plug-ins are additional pieces of software that add extra capabilities to a web browser, such as the ability to view movies and videos, and other types of web content.

Cybercriminals use peer-to-peer (P2P) tools for identity theft.[193] Using P2P tools to share music, software and other digital content is similar to leaving the front door of a house wide open for a burglar to saunter in. A woman's credit card details were found in disparate places such as Troy, Michigan, Tobago and Slovenia because her shared music folder was making her entire "My Documents" folder available to P2P audience for 24 hours a day.[194]

Another key way cybercriminals effectively solicit data illegally is through spamming. The skills deployed vary in their sophistication. An example of a low skill used in spamming involves sending bulk unsolicited e-mails requesting personal details. One example is the notorious 'Nigerian Letter' scam (also called the '419 fraud').[195] This involves e-mails from Nigeria in which the target is enticed to advance sums of money in the hope of realising a significantly larger gain, particularly through high returns from the unsuspecting victim's 'investment'.

The skills for spamming, however, are becoming more sophisticated. Spammers are going back to basics.[196] Nine out of ten spam messages now contain little more than a

[191] John Leyden, (2008), "Cybercrooks get faster, further, nastier," *The Register*, 29th July.

[192] A plug-in consists of a piece of software that interacts with a web application to provide a very specific function "on demand." Applications support plug-ins for many reasons, for instance, to enable other developers to create new applications.

[193] A peer-to-peer (P2P) computer network uses diverse connectivity between participants in a network. Such networks are useful for sharing content files containing audio, video, data or anything in digital format..

[194] Chris Preimerberger, (2006), "Cyber-criminals use P2P tools for Identity Theft, Security analyst Warns." www.eweek.com/c/a/Security/Cybercriminals-Use-P2P-Tools-for-Identity-Theft-Security-Analyst-Warns/, accessed 18th August 2008.

[195] This is also referred to as the "Advance Fee Fraud", named "419 Fraud" after the relevant section of the Nigerian Criminal Code.

[196] John Leyden, (2008), "Cybercrooks get faster, further, nastier," The Register, 29th July. See also Guillaume

few simple words and a web link, which when clicked, downloads malicious code to steal data, according to a survey of major computer company's security division. "Spamvertised sites" also are found in many spam e-mails which contain links to a website or websites, which offer products, ranging from adult entertainment to financial services to health products. The survey also claims that Russia continues to be the biggest single originator of spam (the starting point of 11 per cent of the world's junk). Turkey is second (8 per cent) and the U.S. (7.1 per cent) third.[197]

Slammed for spamming

Facebook, the popular online social networking site, has won an $873 million judgment against a Canadian man, Guerbuez, who bombarded the popular site with sexually explicit spam messages. He fooled its users into providing him with their user names and passwords by using fake websites. After Guerbuez gained access to users' personal profiles, and used computer programs to send out more than four million messages promoting a variety of products, including marijuana and adult toys during March and April 2008. The size of the judgment illustrates how seriously authorities regard spamming.

Source: Michael Liedtke, (2008), "Facebook wins $873M judgment against sex, drugs spammer," Silicon.com. 24th November.

Spammers are also recycling old techniques, such as voice phishing (or vishing). A convincing e-mail is sent to an unsuspecting victim, with all links leading to corresponding, legitimate target pages. But there is a bogus telephone number for recipients to call to reactivate their account, which had been supposedly placed on hold. When recipients call the number they are asked for their bankcard number and PIN, which opens their bank accounts to the fraudsters.[198]

Lovet, 2006). Dirty Money on the Wires: The Business Models of Cyber Criminals. Virus Bulletin Conference, October 11-13, Montreal.

[197] Survey conducted by IBM's X-Force security division, referred to in John Leyden, (2008), "Cybercrooks get faster, further, nastier," The Register, 29th July.

[198] Trend Micro (2008), "Cyber criminals reinvent methods for malicious attacks.

Phishing, now popularly labelled as a *social engineering technique*,[199] is a sophisticated form of spam. Phishing involves attempts fraudulently to acquire sensitive information, such as passwords and bank log-in details, by masquerading as a trustworthy person or business, often from a bank. Bogus e-mails typically invite recipients to click on a link to a fake bank website that has an authentic look. The aim is to lure the bank customers into revealing their pin numbers and other bank account details. The stolen credentials are usually directly sent to the phisher's e-mail address. Other organisations, such as HM Revenue & Customs, are also impersonated in this manner with the same aim. Such attacks have grown exponentially in the last three years.

Phishing attacks have become more sophisticated and daring as cybercriminals are leveraging new technologies and inventing new forms of phishing. One example is targeted spear phishing, which involves higher level skills than those required to send bulk e-mails. Spear phishing is any highly targeted phishing attack in which a fake e-mail is sent to all the employees or members within a certain company, government agency, organisation or group. The message might look like it comes from an employer or colleague who might routinely send an e-mail message to everyone in the company (such as the IT administrator) and could include requests for user names or passwords. Unlike traditional phishing scams which aim to steal information from individuals, spear phishing scams are deadlier as they have the potential to gain access to a company's entire computer system. It just takes one employee or group member to provide their user name or password to open their employer or group to identity theft. Spear phishing also describes scams that target people who use a certain product or website.[200]

Another new form of phishing involves warning potential victims about phishing e-mails as a way to legitimise that e-mail. They are then tricked into clicking on a link that leads to a fraudulent site. Phishers continue to refresh and modernise their trade. For example, over 400 phishing kits designed to generate phishing sites were targeting top

[199] Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. Phishing is social engineering because it tricks people to divulge information, perform certain actions or break security procedures. Trend Micro, (2008), Threat Roundup and Forecast—1H. London, p. 4. See also David S. Wall (2007), *Cybercrime*, Polity Press, Cambridge. Social engineering is also explored in a Whitepaper issued by ENISA (2008) "Social Engineering: Exploring the Weakest Link", The European Network and Information Security Agency.

[200] Microsoft, www.microsoft.com/canada/athome/security/email/spear_phishing.mspx.

web 2.0 sites (such as, social networking, video sharing and Voice-over-Internet-Phone sites), free e-mail service providers, banks and popular e-Commerce websites.[201]Phishing (technical) kits typically bundle all the content required to replicate a targeted website and offer them freely on the Internet.

Cloning the websites of retailers is one quick way to obtain financial and personal data. These cloned websites closely resemble the real ones and require close scrutiny to spot the difference. Another variation is for a request for sensitive information to be posted onto a legitimate website, so that a clearing bank might be seen on its website to be soliciting customer information following a major software malfunction or crash.

Nothing lost but precious data

In December 2005, a group of cybercriminals set up a bogus website claiming to sell a variety of electrical goods at reasonable prices and which stated that it had stock of the 'must have' Christmas gift: a Sony PSP. Over two thousand orders were placed, all providing personal identity information and bank details. Once the details were obtained, prospective purchasers were sent an e-mail advising them that their order could not be processed due to lack of stock. As no money was lost, there was nothing to cause any suspicion on the part of the buyer. It was only when the fraudsters starting using the financial details of the victims a few months later to perpetrate their fraudulent transactions that people felt the impact of the fraud.

Apart from bogus or shame websites used to lure unsuspecting victims, site cloning involves the replication of the look and style of a genuine and trusted website that leads victims to purchase from that cloned website, and lose their financial details to fraudsters with no knowledge that they have done so.

[201] Trend Micro (2008), Threat Roundup and Forecast—1H. London.

"It isn't hard to copy – look at the real Amazon and copy it. If it looks like Amazon, people accept that it is Amazon. They log in as a returning customer so we've got their password too and plenty of people use the same password for everything so that can be handy. Then they get a screen that says they need to put their details in again for security purposes, they press 'click' and that's their name, address, bank details and everything else that we needed sent straight to us."

Source: 192.com, *The Fraudster's Modus Operandi,* p.6.

Criminal gangs have also developed a smart software-based tool to extract and collate the personal data posted on the web of unsuspecting victims. Such data may be used for a multitude of purposes, including identity theft and credit card fraud.

Your CV belongs to us and it's for sale!

Hackers have turned the harvesting of personal information from Monster.com and other large US jobsites into a lucrative black market business.

A Russian gang called Phreak has created an online tool that extracts personal details from CVs posted onto sites including Monster.com, AOL Jobs and many others. As a result the personal information (names, e-mail addresses, home addresses and current employers) on hundreds of thousands of job seekers has been compromised, according to net security firm PrevX.

Phreak has begun selling its 'identity harvesting services' to fraudsters, charging $600 for data that might be applied to targeted phishing attacks, ID fraud or other illicit purposes. Would-be clients are able to contact the gang on special underground forums. For a fee the gang will filter its database for entries that refer to a particular country or particular employer.

The filtering technology is quite sophisticated and smart as it is able to extract and collate only useful data for credit card fraud and identity theft found in CVs, according to PrevX. "Phreak is selling its services to people running higher-end [targeted] spear phishing attacks."

Source: John Leyden, "Trojan trawls recruitment sites in ID harvesting scam," *The Register*, 8th July 2008.

2.2.2 Capabilities and specialisation in the exploitation of information

At the lower end, specialisation in *exploitation* is minimising the level of skills required to perpetrate crime. Some examples are shown below.

Use of non-cyber skills to exploit information.

In a survey conducted in June 2007, the UK's leading online companies revealed that criminal 'shoppers' use their stolen cards to go shopping between 9 pm and midnight because there are likely to be limited staff at this time of the day. About 28 per cent of the companies surveyed declared that this was the period in which most credit card fraud was conducted. [202]

They also tend to buy items in the £250-500 range because these items tend less to arouse suspicion, or merit careful scrutiny by the company's fraud team, or the attention of the card owner or the company issuing the credit card.[203] A recent survey of fraud managers showed that 43 per cent of attempted fraudulent transactions were in the £250 to £500 range and that 29 per cent were in the £500+ range.[204]

Many credit card fraudsters prefer to obtain cards themselves but without stealing them. One way of doing this is known as account takeover.[205] Here, the fraudster manages to obtain sufficient information about the victim to impersonate him or her in bank dealings, in person, by telephone or in writing. The fraudster changes the address associated with the account so that all mail is delivered to another address. The fraudster then gets a new card by reporting the loss of an existing card or requests an additional card.

[202] 192.com Business Services, (2008), *The Fraudster's Modus Operandi*. London, p.10.

[203] 192.com Business Services, (2008), , p.11. Interviews with directors of fraud investigation also say that a main way of detecting fraudulent activity on credit cards is the unusual transaction activity on the card. Interviews were conducted on 11th and 26th November.

[204] 192.com Business Services, (2008), , p.11.

[205] 192.com Business Services, (2008), , p.9.

Upon receipt of the card and the pin the fraudster uses the card. The transactions are not immediately detected because the statement is sent to another address and the victim is unaware of the loss of the card. Only when the transactions become too obvious or high in value will the rightful owner realise that the card has been used fraudulently. "We've got it down to a fine art over the years," boasts an un-convicted credit card fraudster.[206]

Easy, easy, easy

"So I get bank info from purchasers and sort out duplicate cards, either me or the wife goes out and uses the cards to buy anything we want or that we've got orders for and then we just buy stuff that sells well on "auction websites." You learn what goes well by trial and error. My missus does the selling. Then she'll tell the buyer that she needs payment by cheque because of bank problems and offer them a discount for the inconvenience of not using PayPal. The cheque comes and gives us bank details and the name and address of the buyer so it's easy to use that to get duplicate cards and so it starts again… It was a bit of a sideline at first but it's so lucrative that we do it full-time now."

Source: An unconvicted fraudster interviewed by 192.com Business Services, in 102.com Business Services, *The Fraudster's Modus Operandi*, p. 8.

Use of cyber skills to exploit the information.

It is now possible for people with comparatively low technical skills to steal thousands of pounds a day sitting comfortably at home. Credit card fraudsters only need to leave their PC to collect the payment. Sometimes they don't even need to do that if they use wire transfer or e-gold.[207]

[206] 192.com Business Services, (2008), , p.9.

[207] 'e-gold' is a digital gold currency operated by Gold & Silver Reserve Inc. under the name of e-gold Ltd. This company runs a legitimate system which allows the instant transfer of gold ownership between users. e-gold Ltd. was originally registered in Nevis (West Indies) in 1999, but was removed from the register in 2003, due to non-payment of fees. The company claims to have cooperated with the FBI, among other law enforcement agencies in the U.S. Nonetheless, it is apparently an unregistered entity and beyond the jurisdiction of Nevis.

Cybercriminals find e-gold a convenient currency for the following reasons. First, the process is anonymous, quick and uncomplicated; anyone can set up an e-gold account in less than a minute and with a couple of clicks on the computer. No valid e-mail is requested although users are required to have a name, which is not checked. Second, e-gold transactions are irreversible, which means that transactions are final, and the company enforces this policy even in the event of mistakes and; third, the company is independent and beyond the authority of any country.

Many phishing tools are also cheap and easy to use, for instance, a scam letter and scam page in your chosen language, a fresh spam list, technologies to send out 100,000 mails for six hours, a hacked website for hosting the scam page for a few days, and finally a stolen but valid credit card cost about $60 (£40) in 2007. Seemingly the return on investment could easily be 300 per cent, but it could be ten times more.[208] This kind of 'phishing trip' has the potential to uncover at least 20 bank accounts of varying cash balances and will cost only $200 (£134). Details of the data harvested, however, will cost $2,000 (£1340) in e-gold if they are sold to another cybercriminal.[209] Nevertheless prices are far from static in underground markets. Rapid changes in prices are the result of the exponential growth in the supply stolen data. Recent research indicates that the market for stolen personal information, including credit card details, and personal information has grown to such an extent during 2008 that prices have fallen dramatically ranging for credit card details from $0.06 (4p) to $30 (£20) and full identities from $0.70 (46p) to $60 (£50).[210]

New technologies also make the replication of genuine documents easy and of a high enough standard to escape scrutiny. For instance, a counterfeit driving license could be used to authenticate identity and address for the purposes of store credit. Such counterfeiting sites are available on the Internet.

Guillaume Lovet, (2006), Dirty Money on the Wires: The Business Models of Cyber Criminals. Virus Bulletin Conference, October 11-13, Montreal.

[208] Guillaume Lovet, "How cybercrime operations work – and why they make money." http://www.out-law.com/page-7791 (accessed 29th November 2008).

[209] ibid

[210] Prices varied according to the amount of information included with the card or identity, rarity of the information, and bulk purchase sizes. Symantec (2009) Symantec Global Internet Security Threat Report, Trends for 2008, Volume XIV, Published April 2009.

The trend towards the development and marketing of user-friendly tools for criminal exploitation is rapidly developing into crimeware-as-a-service (CaaS, see below). The emergence of crimeware as a service releases criminals from having to deal with the technical challenges of cybercrimes.

Some of these services include crimeware toolkits. As noted above, these provide readymade tools for criminals to gather and sort out the data stolen, minimising the necessary coding skills to operate them.[211] The director of security strategies from a large IT multinational said "for subscriptions starting as low as $20 per month, such enterprises sell "fully managed exploit engines" that spyware distributors and spammers can use to infiltrate systems worldwide.[212] It is likely that CaaS will increasingly hamper the ability of law enforcement to track malicious hackers.

One respected commentator has argued that the virtual relationships within online communities "[…] encourage the social deskilling of the individual through the specialisation and compartmentalisation of interactions."[213] However, the examples presented above suggest both increasing acquisition of technical skills and deskilling, depending on the type and activity of cybercrime. Consequently, capability is being spread across a dramatically increasing range and number of users. Highly capable cybercriminals are developing skills that will harvest data worth vast sums of money. However, a barely capable but dogmatic cybercriminal can still make an effective living with a small investment of funds and limited computer literacy.

The cybercriminal ecosystem frames the environment in which networks of criminals specialise, cooperate and compete with the ultimate goal of generating an illicit profit. Their interconnection and dependence means that to pursue their individual interests, they need to became part of value chains, where different actors specialise, link and upgrade, driven by innovation. A wide variety of actors participate in the cybercrime

[211] Finjan, (2008): Web Security Trends Reports, Q1.

[212] Gunter Ollman quoted at: www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9015588.

[213] Wall, D. (2007), Cybercrime: The Transformation of Crime in the Information Age, Polity Press, UK, p.33.

ecosystem at various levels, creating different business models. Some of these are explored below.

2.3 Cybercrime business models

Mimicking legitimate commercial businesses, cybercriminals in the underground economy operate on a free market principle applying principles such as volume discounts, commissions and pay as you go services.

The third component of the cybercrime digital ecosystem is that of business models. The position of firms and their activities in the value chain helps determine how it approaches business and generates a profit; all definitions of business models emphasise how firms make money. Business models have the added attraction of being potentially comparable across industries. Therefore, for this study, business models will refer to the way in which different cybercriminals specifically generate revenue, and the nature of the arrangements they have with their suppliers and customers in the value chain. Suppliers and customers will vary depending on the activity in question. For instance in 'infection and distribution' malware writers would be the suppliers of malware to their customers, the botnet owners. However, in 'exploitation' activities, botnet owners may supply buyers with stolen credit card details.

In any given industry, the methods of doing business may vary between actors and over time. Alternative ways of conducting business can arise and change with new technologies, market opportunities and competition.

There has been much speculation about the level of organisation and professionalism of cybercriminal organisations. While too little is known about the types of business models that operate in the underworld, we do know that all cybercriminals want to make money. We also know that every business model has its own inherent strengths and weaknesses. This section intends to categorise business models in cybercrime to establish a base from which to examine their potential weaknesses.

While some models are quite simple, other can be more intricately woven. This preliminary study has identified three predominant business models that are briefly introduced below: off-line business models, Internet-based business models and hybrid models (combining the other two). Since most cybercrime activities take place online, Internet-based examples are more numerous. However, a significant component of

cybercrime activities takes place offline, as well as a combination of online and offline methods. Examples of these types of cybercriminal operations are captured in the sections below.

2.3.1 Offline business models

Although the Internet is a common meeting and workplace for cybercriminals, we have seen that some credit card fraud and ID theft still takes place in a traditional offline fashion. These activities are usually higher risk, since they lack the anonymity of the Internet. However, they have provided an opportunity for traditional crime gangs to exploit the economic opportunities of cybercrime businesses benefiting from their existing structure, hierarchy and occasional funding from other illicit activities. Some of the business models identified as a result are the loyalty business model and business process outsourcing.

The *loyalty business model* is used in strategic management where company resources are employed to increase the loyalty of customers and other stakeholders to meet corporate expectations. Whilst supermarkets might use loyalty cards, organised crime groups may maintain the loyalty of gang members and the code of silence with cash 'incentives'[214] or the threat of violence or extortion. These are at the root of the offline criminal ecosystem, which requires more established criminal practices than online criminality, and are a reminder of the negative, dishonest and violent connotations that largely define this ecosystem.

The *business process outsourcing* (BPO) involves contracting operations and responsibilities of specific business functions (or processes) to a third-party service provider. It is traditionally associated with large manufacturing firms outsourcing large segments of their supply chain. Today, it is primarily used to refer to outsourcing services. In the cybercrime business, given the variety of technical and organisational skills required to perpetrate certain crimes, many of the services are hired or outsourced. It is well reported[215] that criminal organisations are increasingly hiring financial specialists to conduct their money laundering transactions in countries where financial jurisdictions are "safer". Similarly, criminal gangs can easily hire the technical

[214] Council of Europe (2005): Organised crime situation report; Focus on the threat of economic crime.

[215] MacAfee (2008), "One Internet, many worlds".

expertise they need to perpetrate one type of attack, ensuring – through a mixture of rewards and threats – that the technical expert will conduct the assignment effectively.

2.3.2 Hybrid business models

A hybrid business model results from the combination of physical (off-line) and web channels (online). Many authors have differentiated hybrid models from Internet-only businesses models, using terms like 'bricks and clicks', – also known as 'clicks and mortar', 'surf and turf, 'cyber-enhanced retailing', 'hybrid e-commerce'[216] – and swarming business models.

The bricks and clicks business model and its variations generally describe the partnership between Internet businesses and traditional distribution companies – for instance the successful business model adopted by Amazon, where orders placed online are physically distributed by the postal system. In the cybercrime business, the integration of e-commerce with physical channels takes place mostly at the lower end of the value chain, that is, during the final transformation of stolen information into cash, without which the entire process would have no meaning or value. The business model of drop services provides an example of a combination of web channels of communication with the purchaser of illicit goods online, and off-line provision of a physical address to mail the stolen goods.

The Swarming business model involves the temporary collaboration of individuals to meet a particular challenge or goal. In the legitimate world, members of the 'swarm' work towards a collective interest, which is broadly defined by any of the stakeholders and is driven by innovation.[217] Many legitimate businesses have used collaborative

[216] Timmer, P., (1998), "Business Models for Electronic Markets", Electronic Markets, 8 (2), 3-8,; Otto, J. and Q. Chung (2000), "A Framework for Cyber-Enhanced Retailing: Integrating e-commerce Retailing with Brick and Mortar Retailing", Electronic Markets, 10 (4), 185-191; Afuah, A. and C. Tucci (2001), "Internet Business Models and Strategies: Text and Cases", New York, NY: McGraw-Hill Irwin.; Steinfield, C., T. Adelaar, and Y.-j. Lai (2002), "Integrating Brick and Mortar Locations with E-Commerce: Understanding Synergy Opportunities", Hawaii International Conference on Systems Sciences, Big Island, Hawaii, January 7-10.

[217] Gloor, P. A. (2006). Swarm Creativity: Competitive Advantage through Collaborative Innovation Networks. Oxford; Gloor, P. A. and Cooper, S. (2007). The New Principles of a Swarm Business. In: MIT Sloan Management Review, Nr.: 3, S. 81-84.

innovation networks to facilitate close cooperation between customers and product developers. In the cybercrime industry 'swarms' can be born online – similar to what we call below the 'Internet community business model' – but in most cases they combine physical and online means for communication (online collaboration among individuals who also meet in person). One distinct feature of the model is that swarms generate for a specific purpose and for a limited period of time, until the goal is achieved (unlike the Internet-based model). Although it is based on commitment and loyalty to achieve a specific goal, this business model also lacks managerial hierarchy or the proprietary ownership of ideas that is a feature of the loyalty model. Whilst there may well be a swarm-type interaction that requires the major stakeholders to physically meet from time to time, pure cybercriminals have no need for this business model as they have built up anonymous and highly effective channels of communication that do not require and even eschew face-to-face meetings and the negotiation of common cause beyond cyberspace.

2.3.3 Internet-based business models

The growth of Internet-based businesses in the legitimate world has resulted in many classifications and methods of conducting business over the Internet. E-commerce has given rise to new kinds of business model. The benefits for customers and suppliers offered by online businesses over physical channels have been highlighted by many commentators, and include reduced operational and overhead costs, scale and scope, access to wider markets, lower inventory and building costs, flexibility in sourcing inputs, improved transaction automation and the ability to bypass intermediaries. Cybercriminals benefit from all these advantages as well as enjoying anonymity. The Internet provides criminals with a favourable environment to disguise their identity, even amongst trusted colleagues, making them hard for law enforcement agencies to locate.

Some models identified in our initial search include:

Advertising-based models: This model is used quite legally by companies that provide content or services to visitors and sell advertising to businesses that want to reach those visitors. The advertising based model is widely used by IRCs and web forum operators. In the underground economy, advertised items include bundles of credit card numbers, identity theft information, online banking information and skilled labour, where discounts

are often offered for bulk purchases.[218]Advertisers on underground economy servers are usually self-policing and report 'rippers'[219] to the server administrators.[220] IRC administrators and operators, the people who provide and run the network, generally do it on a voluntary basis – which differentiates their operations from a commission-based model. However they also advertise and benefit from the information shared in the IRC. There is no overlap or interface between the legal and the illegal advertising-based models.

Brokerage model: At the heart of the brokerage model are third parties known as brokers, who bring sellers and buyers of products and services together to engage in transactions. The broker usually charges a fee to at least one party involved in a transaction, sometimes both. There are various types of brokerage business model, such as the auction broker and the transaction broker.

a) The use of the traditional auction brokerage model is now widely used online and expanded to more goods and services through the basic backing of a commissioned brokerage agent. For instance eBay is an example of legitimate auction site where the broker charges the seller (individual/merchant) a listing-fee and commission based on the transaction's value and according to varying terms of the offering and bidding. In the cybercrime business auction fraud is an ordinary practice where the victim will then send money to pay for the item on which they bid, but they will never be sent the actual item in question. This type of fraud can be especially difficult to prosecute since the offender and victim may be located in different countries. Identity theft is another problem surrounding online auctions, and in many cases fraudulent transactions are used to steal financial information from the victims. In this model, cybercriminals simply exploit the weaknesses of the legitimate model.

b) The transaction broker provides third-party services for buyers and sellers to settle their payment transaction. The goal of the broker is to ensure that the customers obtain

[218] Symantec (2008), "Symantec Report on the Underground Economy", July 07–June 08.

[219] Rippers are members of the fraud community who steal from other members by reneging on agreements to provide cash for stolen data or simply keep the data without paying the provider. See www.symantec.com/norton/cybercrime/blackmarket.jsp.

[220] Symantec (2008), "Symantec Report on the Underground Economy", July 07–June 08.

some advantages from conducting their financial transaction via their site. A legitimate example is PayPal – this service allows financial transaction between buyers and sellers without sharing financial information and gives them the flexibility to pay by card or cheque. In the underground cybercriminal business this would be illustrated by the providers of referral services. These specialised services act as a 'trusted' intermediary between a seller and buyer of malware and other illegal services. Such agents hold the money on the transaction until a buyer has had a chance to check that the goods or services purchased function as promised. Their fees can range from 2 per cent to 4 per cent of the total transaction.[221]

Internet community model: This business model is based on the creation of a virtual community of interested users who support the development of products through voluntary donations. A legitimate example is the 'Open Source' community. Sourceforge, the world's largest repository of Open Source software development projects, has over 170,000 registered projects and nearly two million individual users.[222] The growth of Open Source has provided an organising structure for many user-led projects together with a set of guiding principles and a language to describe what they are doing. Some projects, like Linux and the Apache web server, have helped to re-shape the global IT industry, whilst others have had a similar effect on music, video games, education and health. The sheer volume of Open Source activity is a strong indicator of the growth in hacking skills, and there is evidence that communities of hackers are developing attacking tools mimicking Open Source communities. There are examples such as the distribution of Try2DDoS, a tool that automates distributed denial of service attacks. It was first released in June 2005 on Underground Konnekt, a French hacker website. Over the next two years, identical source code turned up in China, Guatemala, Russia and Argentina. As the programme moved around the globe within the online community of hackers, the tool gained new capabilities, including support for Spanish and Chinese languages.[223] The community of 'users' play a critical role in fostering innovation in this business model. There is also the opportunity for revenue to be generated around open source from related services such as systems integration, product support, tutorials and user documentation.

[221] Symantec (2008), "Symantec Report on the Underground Economy", July 07–June 08.

[222] http://sourceforge.net/, accessed May 16, 2008.

[223] Dan Goodin, (2008), Online crime gangs embrace open source ethos: Malware gets globalized, 17th January 2008; www.theregister.co.uk/2008/01/17/globalization_of_crimeware/.

Crimeware-as-a-Service (CaaS): Parallel to the concept of software-as-a-service,[224] crimeware-as-a-service is rapidly gaining attention in the underground economy. Using CaaS, criminals can now rent malware and hosting services along with any patches needed to defeat security software. The final user only needs to have a target and to identify the type of data they seek to steal, while the technical work can be hired. The emergence of CaaS releases criminals from having to deal with the technical challenges of cybercrime. Under this business model, everything can be rented, from crimeware toolkits to pay-per-infection services.

a) *Crimeware toolkits* offer off-the-shelf tools that allow criminals to gather and sort out the data stolen, minimising the need for coding skills to operate them.[225] One director of security strategies for a major corporation said "for subscriptions starting as low as $20 (£13.40) per month, such enterprises sell "fully managed exploit engines" that spyware distributors and spammers can use to infiltrate systems worldwide.[226]

b) *The pay-per-infection model* emulates the 'pay-as-you-go' approach, based on actual usage rates. These businesses sell other criminals code that enables them to infect websites with malware or spyware. One interviewee found a website that was initially charging €40 (£35) each time the spyware was downloaded to personal machines; however, the site offered more favourable rates when the traffic increased.[227]

Business models are not independent from each other; they often combine. For instance, the swarming model – where participants work together on a common goal - can also include crime-as-a service elements. Many sources have discussed and made

[224] Software as a service (SaaS) is a model of software delivery where an application is hosted as a service provided to customers across the Internet. This model is centred on separating software possession and ownership from its use. Turner, M., Budgen, D., and Brereton, P. (2003). Turning software into a service. Computer, 36(10), pp 38-44 (October).

[225] Finjan, (2008), Web Security Trends Reports, Q1.

[226] Gunter Ollmann, at IBM's Internet Security Systems X-Force team quoted at: www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9015588.

[227] Finjan, (2007), eCriminal eCommerce and the Web Models and Techniques Used to Support it, Baptie Online; by Tim Warner, UK Country Manager, Finjan.

assumptions about the various types of business model and their features but have failed to demonstrate how much cybercrime falls into each category. However, with the fast adoption of the Internet, online business models have proliferated in recent years. Our interviews have largely supported this view, and made an important call to improve both the general understanding and the necessary technical knowledge to prosecute Internet-based business models – since current efforts seem to be placed in traditional offline and hybrid methods.

3 Conclusions and recommendations

3.1 The future trends for cybercrime

Involvement in cybercrime is likely to continue on the path of low risk and high gain. New business models and new entrants encouraged by low barriers to entry are already emerging.

The organisational and technological capabilities of cybercriminals, particularly with no global counter-strategy, will likely go deeper and wider into the foreseeable future. As cyberspace develops further, new opportunities will open up.

It remains to be seen how the current global financial crisis will affect this situation. If it is deep and prolonged, this may hit the emerging and educated middle classes in developing countries harder than most and encourage a new generation of under- or unemployed youth with IT skills to seek entry into the profitable and comparatively low risk world of cybercrime. The BRIC countries have already seen the start of such a growth. Countries in South East Asia, the Middle East and Central and Southern Europe cannot be too far behind the further extensive diffusion of IT capabilities into Africa, Asia, Latin America and parts of Europe.

As more countries gain substantial economic power, global solutions to global problems will become more difficult to attain – genuine, broad based consensus will replace the viewpoint of a single superpower. In the absence of effective global governance and leadership, loose networks will proliferate to pursue convergent goals and interests.

This can also be seen within the cybercrime ecosystem and, moreover, the ecosystem perspective permits a clearer view of multipolarity within the cybercrime universe, with

no dominant force. Unlike traditional organised crime models, ethnicity appears to be neither a barrier nor an advantage. Cybercriminals will make common cause with anyone where such links are of mutual benefit. Age, sex, religion, location, ethnicity all seem to be irrelevant which could define the world of cybercrime as a pure form of meritocracy. As the opportunities for qualitative and quantitative expansion occur, the only barrier to entry will be the skills required. The implications for victims, analysts and law enforcers could not be more daunting.

Crimes such as electronic theft and fraud will occur more rapidly, reducing the likelihood of being caught. Information about how to compromise a system will be available more quickly and to more people, which means that opportunistic criminals linked into organised networks of will no longer be controlled by organised crime – if indeed they ever were - and these components will come to dominate and define the ecosystem.

The education and ability of criminals to use new technology will also have a major impact on the nature of crime. In cyberspace, we can expect this to be further magnified. The relationship between the offender and victim may change, as neither sees the other as a person. The lack of such awareness may see online offenders committing more extreme crimes. Equally, if victims have no contact with the offender, their attitudes to punishment may change. Whether this will see a reduction in demands for punishment, or an increase in those for harsher penalties, is not clear.[228]

The constraints upon cybercrime are unlikely to be as comprehensive as for some other forms of crime. Whereas narcotics and human trafficking have immense implications for the welfare and safety of vulnerable groups, this is not perceived to be the case with low level fraud. When identities and credit cards are stolen, the relevant authorities tend to react quickly to replace and compensate. As such, the resources available to law enforcement agencies will tend to be channelled into programmes to combat the types of illegal activity that pose the greatest threat to vulnerable groups. Therefore, the environment in which cybercriminals operate is likely to remain benign and increasingly attractive to a growing number of people, not least from within states and regions where law enforcement is weak.

[228] Davis, R. and K. Pease, (2000), Crime Technology and the Future, Security Journal, p.62.

Both the international system and its component parts lack the comprehensive instruments to tackle cybercrime in all its forms. And there is no evidence that they are doing anything about it. The growing immunity for cybercriminals and the promise of easy gains against a backdrop of global recession will surely fuel the supply side of what threatens to become a global criminal industry.

But we do need to respond and we need to do so at three levels: international, national or institutional, and individual.

3.1.1 The international level

Across the world, cybercrime will continue to offer high rewards and low risks both to organised and to opportunistic criminals. New players are emerging in countries like India and Brazil and as international financial networks acquire a greater global reach, such opportunities will multiply. The international response has been weak, given the scale of the problem, and there are no signs of preparation to withstand a future cybercrime onslaught.

Countries do face problems responding collectively in an appropriate and effective manner. The scale and nature of the problem is genuinely transnational – credit card details stolen in the UK can be processed in Malaysia and used in Australia, while Indian call centres are thought to be a source for insider fraud.[229] Some of the states involved are failed or weak states and are unlikely to be able to respond even if they wanted to do so. Although several international organisations have had cybercrime on their agendas (including the OECD, European Union and G-8 group) they have yet to achieve consensus and traction on dealing with the problem. As yet, no one state has opted to take the lead to develop the necessary architecture and political consensus to mount a sustained campaign against cybercrime. Neither of the two Protocols that constitute the Palermo Convention, for example, address any issues relating to cybercrime. The international policing organisations, INTERPOL and EUROPOL have yet to develop robust responses. The European Union did manage to draft a convention on cybercrime in 2002 but, to date, not all member states have ratified the agreement. Moreover, where action

[229] As noted in section 2.2.

is taken, priority is understandably given to issues like child pornography, though this means resources are not available to tackle financial cybercrime.

3.1.2 The national level

At the national level, law enforcement agencies are ill-equipped to address cybercrime. Funding is woefully inadequate and unlikely to rise to acceptable levels in the foreseeable future and clear decisions have to be taken over priorities. The creation of the UK Serious Organised Crime Agency (SOCA) was a bold move, insofar as it attempted to go beyond traditional law enforcement responses by deploying intelligence specialists as the senior executive officers. But its successes have been limited which is why an E-Crime Unit was established. However, the E-Crime Unit appears underfunded and unlikely to be resourced to anything close to an adequate level considering the scale and nature of the problem. The problems associated with cybercrime clearly require urgent attention at a ministerial level. The E-Crime unit has a budget of only £7 million for three years and the City of London Police, who have national responsibility for credit card and cheque fraud, only have thirteen officers to cover the entire country. Although highly professional and committed, there is little or no capacity to do anything more than attempt to enforce the law after crimes have been committed and if they are over £20,000. There appears to be little or no response possible regionally or locally due to the lack of resources and expertise.[230] An individual who has been the victim of credit card fraud will first be requested by the authorities to contact their bank or card company, not least to ensure compensation. Data capture and analysis remain firmly in the domain of the private sector and the role of the police is largely restricted to limited enforcement, purely on the basis of resource constraints.

By the autumn of 2009 the new National Fraud Reporting Centre (NFRC) should allow for the differentiation of different types of cybercrime. However, even then the underreporting of private data breaches is likely to mean the data collected will be inaccurate. This has been a recurrent critical concern raised by the majority of our interviewees, including IT security firms, IT experts, academics and the police. This view was also expressed by the House of Lords Science and Technology committee in 2007 in its personal security report: "a data security breach notification law would be among the

[230] Interviews with police suggested that until such time as financial cybercrime becomes a political priority, it is unlikely to be assigned adequate resources by chief constables with limited budgets.

most important advances that the UK could make in promoting personal Internet security".[231]

In both Europe and the UK, there have been many proposals over the last five years for legislative change that would force firms to notify regulators and customers of all breaches of their data security. Many voices have come out in favour of enacting data security breach notification laws (UK NGOs[232] and The European Data Protection Supervisor – EDPS).[233] In the UK, there were encouraging signs when the Information Commissioner's Office (ICO) suggested that the revisions to the EU's ePrivacy Directive "could be the "catalyst" needed to get data-breach notification into UK law" in July 2008.[234] However, by November, the UK government announced that it would not be implementing a data-breach notification law, similar to the existing one in the US. This stance could put the Government at odds with the European Union, which plans to force companies to own up to data breaches as part of its new ePrivacy Directive.

By contrast, 44 US states[235] had enacted legislation by December 2008 which requires notification of any security breaches involving personal information from public and private organisations. Legislation on data breach notification was first passed in California in 2003.[236] In general, most state laws follow the basic tenets of California's original law: companies must immediately disclose a data breach to customers, usually in writing. Also in California, there is a private right of action, and there are very few exemptions.[237]Since the adoption of this legislation in a majority of US states, reports of security breaches have rocketed and breaches from private companies are regularly reported. In the UK it has been argued that the US experience has not been a

[231] House of Lords, 2007, Personal Internet Security Report, p 57.

[232] For example silicon.com, who launched a Full Disclosure campaign in 2007.

[233] The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good data protection practices within the EU, both by monitoring the EU administration's own data processing, as well as by commenting on pending legislation.

[234] Heath, N. (2008) "ICO:Data breach law moves closer", www.silcon.com, 3/7/08.

[235] Plus the District of Columbia, Puerto Rico and the Virgin Islands.

[236] Data breach disclosure law, SB 1386.

[237] Law in some other states allow more exemptions or do not allow a private right of action. For instance, California allows exemptions for encrypted data that's lost and publicly available government data. In California there is no such thing as an immaterial breach, while other states do have a definition of immaterial breach.

particularly good one, since constant reports of breaches have the potential to desensitise the public to data losses.[238] However, the European Commission – as well as many interviewees – consider that such a regulation would create an incentive to invest in security (EC, 2006).

UK Government departments are the only bodies required to notify the information commissioner of any potential data losses. This requirement does not apply to private business, so the extent of the problem remains largely unknown. In the absence of legislation, the commissioner has produced guidance for businesses on when it should be notified of data breaches as a matter of good practice.

But one event on the horizon makes action imperative. The 2012 Olympic Games in London raise serious issues and challenges in relation to cybercrime. Cybercriminals have in the past exploited high-profile events either for financial gains or to lure unsuspecting web users into downloading malicious code. The experience from previous Olympics tells us that the number and scale of cyber attacks increase at each event. The Sydney Olympics lost £500 million in contract fraud. The winter Olympics in Turin 2006 had four million attacks per day (though only 49 required immediate action).[239] In Beijing 2008 the number of attacks rose to about 12 million security alerts per day, with alarms triggered on more than 12,000 devices spread over 70 venues.[240]

The London 2012 Games have been tagged as the first 'digital Olympics' by one of our interviewees. Digital technologies will be an integral part of the ticketing, billing, broadcasting and transport systems. The IT infrastructure for London Olympics supersedes the complexity of any previous Games – about 900 servers, 1,000 network security devices and 8,000 computers will be provided.[241] Video streams, real-time Games updates and live travel information will be accessible from mobile devices. Blogging and social networking are also intended for interaction between athletes,

[238] Data Sharing Review Annex Report, Ministry of Justice, 2008.

[239] Interview with Michael Hallowes, National Policing Improvement Agency (NPIA), 2nd April 2009. It is, however, recognised that such aggregated data makes no differentiation between a deliberate external attack from an unauthorised use of a USB port to re-charge a mobile phone.

[240] Nick Heath (2008), "Protecting the Beijing Olympics from hackers. How IT experts kept the Games on track", Silicom.com, 30th October 2008.

[241] Nick Heath (2009): "Olympics IT gets lean, mean and green", Silicom.com, 5th March 2009.

spectators and the media.[242] Even the transport system will be automated through Oyster cards. More than ever before, the London Games are expected to fuel an explosion in internet traffic of online transaction and activities. And this represents the most complex logistical challenge for the UK.

The great opportunities brought by digital technologies are accompanied by great risks, through greater vulnerability. Risk management and preventive measures will require considerable resources and technical capability for which the UK is not fully prepared. There is little evidence that the capacity of the UK to host the Olympics matches the threat in cybercrime.

Capacity to deal with these problems needs to be built up now, with an increasing involvement of the police in tackling credit card fraud and ID theft.

3.1.3 The individual/institutional level

Many of the opportunities presented to cybercriminals are the result of human error and a poor appreciation of the need to protect personal data. Too many people use a single password or the same 'memorable information'. Even those who are aware of good practice in protecting personal data often ignore appropriate procedures in favour of ease of use. Most individual computer users are unlikely to know the latest advice until their data or money is stolen. As new social engineering techniques are devised and more sophisticated forms of malware developed people do need to become more aware of how they can protect themselves.

At the institutional level the risks can be multiplied many times given the general lack of security training and screening in most companies and organisations or the potential for disgruntled or dishonest employees either to ignore or subvert company policy.

Organisations and initiatives such as the National Computer Centre, the European Network and Information Security Agency (ENISA), Get Safe On-line have excellent programmes and advice on how to increase our personal on-line security. Such laudable initiatives are often joint efforts by government and the private sector. But their

[242] John O'Brien (2008): "London 2012: Will IT be hit by credit crunch?", Silicom.com, 9th October 2008.

outreach needs to be evaluated to ensure that the public is aware of their efforts and to assess their effectiveness.

Another way to improve personal and institutional security would involve further development of systemic or individual privacy enhancing technologies (PETs). These require investment, foresight into the likely direction of criminal activities (via search techniques, scenario exercises, etc.) and public debate about privacy and data protection.

However, some cybercrime experts believe that much of the technology is in fact secure and in place and it is mainly human error and insider subversion that accounts for breaches of security.

3.2 Recommendations

There is clearly the need for action at all three levels by the state, the private sector, the research community and the individual.

As the current recession deepens, cybercrime looks set to make an even greater impact due to a conjunction of factors. First, increasing unemployment could drive more people into committing cybercrime. The E-crime Survey 2009 reported that fraud committed by managers, employees and customers in 2008 tripled compared to 2007. [243] It is reasonable to assume that the recession will exacerbate those problems. Second, the recession is shrinking the liquidity of banks thus limiting their ability to compensate the financial loses of victims. Finally, upcoming dramatic reforms in the police structure may reduce the size of police forces and lead to more cost-effective measures. One of our interviews[244] suggested that there is an urgent need to change the way information is collected by the police. Effective collection of data associated to cybercrimes and sharing information nationally across police units and internationally – with EUROPOL, and INTERPOL– is one high-impact measure that could be implemented with relatively little money, since information is already shared internationally for other internationally distributed crimes, such as terrorism.

[243] KPMG (2009), "E-Crime Survey".

[244] Interview with Michael Hallowes, National Policing Improvement Agency (NPIA), 2nd April 2009.

In the UK a national initiative is urgently required, which is followed up at a regional level and in international forums. The UK should co-ordinate the national fight against cybercrime in partnership with other international actors. For this purpose, combining resources and sharing information across national, regional and international intelligence forces becomes crucial. European Union member states need to make common cause.

Given that so many cybercrime operations take place in developing countries, aid agencies need to be persuaded to become significant stakeholders – having already become involved in police reform programmes, this is an institutionally legitimate area of development.

The value chain analysis illustrates the disperse nature of cybercrime – multiple actors involved in the processes of detecting vulnerabilities, infection, distribution and exploitation – which makes it difficult to identify the criminals. Once crimes are perpetrated, there is a question as to who bears the costs? In this process, the victims of cybercrime – often individuals – tend to become powerless receiving mixed information from police, banks or retailers. One of our interviewees[245] strongly recommended that the protection of citizens needs to be at the heart of any new initiatives to combat cybercrime.

The fundamental problem within the private sector is transparency. Simply put, the high street banks have been reluctant to release adequate information. The recent, fundamental shift in the relationship between these institutions and government as a result of the financial crisis should be used to apply leverage to encourage greater information sharing and analysis. It is also unclear to what extent the banks work together in this area but there is a strong suspicion that efforts are atomised, whereas cooperation would offer a far better use of resources. Banks should also be encouraged to pledge a percentage of profits or turnover to combating cybercrime.

A similar response is required in relation to the independent security firms that track and analyse cybercrime. There is little transparency with regard to capabilities and methodologies. In the absence of such information, there is a tendency to suspect that

[245] Interview with Michael Hallowes, National Policing Improvement Agency (NPIA), 2nd April 2009.

some of these firms may have adopted methodologies and techniques that inflate the scale of the problem and the level of vulnerability, not least as a means of generating business. Here again, government intervention is required to develop a code of practice for the private sector which could be enforced by an Ombudsman.

Both the private and the public sectors are increasingly looking to the policy research and academic communities for a greater input into understanding and analysing cybercrime, especially with regard to 'over-the-horizon' perspective. Although cybercrime research is now an accepted criminology sub-discipline, it remains in a developmental stage. More criminologists (and IT experts) need to be trained in this area, although it has begun to attract the attention of the UK research councils.[246] At the regional and international level, genuine institutional partnerships and networks need to be forged, developed and maintained. There is an urgent need for research on the different approaches that individual countries have taken to combat cybercrime.[247]

As is often the case, efforts to combat cybercrime would be greatly enhanced if greater collaboration and co-ordination could be achieved; in policing, this would seem to be the main raison d'être for the creation of the E-Crime Unit. However, co-ordinated activities need to be looked at across the board. Financial cybercrime is increasing exponentially. In due course it will begin to affect a global banking system already severely weakened by the global financial crisis. The system cannot continue to mask the scale and nature of the problem by compensating, in good faith, the victims of theft and fraud (and then presumably passing on the costs to their customers). Co-ordination and collaboration can make the best use of the limited resources available that may not increase in the future to anything like the level required.

Our research has clearly indicated that there is no technical fix available. One of the most difficult policy areas concerns individual lapses in personal security – the human dimension.

[246] The UK's Technology Strategy Board has recently begun to devote funding for the creation of centres for the development of security technologies.

[247] France, for example, is thought to have fared less badly on account of relatively strict state controls over the overall banking system, whereas the US banking system is particularly vulnerable.

Responses are required at all the levels identified above. As individuals we need to retrain ourselves to make our personal IT systems more secure, although there is little incentive if banks make good cybercrime losses in such an efficient way, creating minimal inconvenience for the customer.

The private sector responses should be reviewed and analysed in search of best practice. The security forces should work together in areas currently defined by insularity. The international system must pool resources and information. Cybercriminals operating in weak states require a major effort as effective responses cannot be expected to occur without help from multilateral agencies and the more capable law enforcement bodies. Research initiatives should also be genuinely multidisciplinary, to include, for example, criminology, development studies, economics (finance, micro-, macro-), IT studies, innovation studies and, even, strategic studies.

Additional resources will be increasingly difficult to secure given the state of the public finances; yet levels of funding to address cybercrime in the UK and elsewhere are already derisory. However, this is not a lost cause. The relatively cash rich development sector should be brought in as a major stakeholder, not just for resources but also for expertise. When the banking system recovers, it should be asked to provide more resources, which should presumably be easier now that so many are all but nationalised.

The challenges are to seek a reorientation of existing resources and capacity and to begin with initiatives that are less resource intensive – transparency is mainly a result of attitude and good practice. As such, the UK government has a leading and major role to play, which should be cross departmental in scope to include the Home Office, FCO, DfID and even the MoD – combating cybercrime in all its forms is a compelling argument to revisit the need for 'joined-up-government'. The Cabinet Office should take the lead in co-ordinating strategy and policy across government.

There are many worrying estimates over just how extensively cybercrime has already accessed financial information and possibly not all are exaggerations. If even a small percentage of the estimates turn out to be correct, there are more serious problems on the horizon. At present, a 'band-aid' response has prevailed but nobody has really taken on the task of working through what might be the implications if the patient becomes too ill for band-aids to work. Against a backdrop of recent financial meltdown, the effects of which will weaken the overall system for many years to come, lower levels of

resilience must now surely be of concern. Sound analysis of the extent of our systemic insecurity and vulnerability could offer a starting point to place the scale of the problem in perspective.

Appendix

Glossary for cybercrime

(The definitions in this glossary were gleamed from numerous sources including the BBC News and Wikipedia.)

1) **Adware**: unwanted programs that, once installed, bombard users with unwanted adverts. Often those pushing the adware programs get paid for every machine they manage to recruit. Some adware poses as fake computer security software, and it can be very hard to remove.

2) **Blackhat hackers:** also known as 'Crackers', are hackers, who use their skills for explicitly criminal or malicious ends. They penetrate systems and often modify and/or destroy data. The terms used to refer to writers of destructive viruses or those that use attacks to knock websites offline. Now it is likely to refer to those that steal credit card numbers and banking data with viruses or by phishing.

3) **Botnet**: the word is generally used to refer to a collection of compromised computers (called 'zombie' computers or 'bots'— as abbreviation of 'robots') running software, usually installed via worms, Trojan horses, or backdoors, under a common command & control infrastructure, controlled by a single person. The majority of these computers are running Microsoft Windows operating systems, but other operating systems can be affected. The biggest botnets can have tens of thousands of hijacked computers in them. Recent research suggests they can be hired from as little as 4 cents per machine.

4) **Botnet herder**: one of the names for the controller or operator of a botnet.

5) **Carder**: someone who steals or trades exclusively in stolen credit card numbers and their associated information.

6) **Cash-out**: a euphemism for stealing money from a bank account or credit card to which someone has gained illegal access. Hackers who grab credit card data often do not possess the skills or contacts to launder the money they can steal this way.

7) **Click fraud**: also called pay-per-click fraud –the practice of artificially inflating traffic statistics to defraud advertisers or websites that provide venues for advertisers. Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.

8) **Crackers**: see definition of blackhat hackers.

9) **CVV2**: is a three or four digit value that is uniquely derived for each credit card and is found at the back of the card. It is a new authentication procedure established by credit card companies to further efforts towards reducing fraud for internet transactions, since it attempts to verify to the merchant that the cardholder does in fact have the card in his or her possession.

10) **DDoS**: abbreviation for Distributed Denial of Service. This is an attack in which thousands of separate computers, which are usually part of a botnet, bombard a target with bogus data to knock it off the net. DDoS attacks have been used by extortionists who threaten to knock a site offline unless a hefty ransom is paid.

11) **Drop services**: online money laundry service, where someone sets up anonymous mailboxes and has people send goods purchased with stolen card details for a certain fee, and then ship it off to the customer.

12) **Exploit**: a bug or vulnerability in software that malicious hackers use to compromise a computer or network. Exploit code is the snippet of programming that actually does the work of penetrating via this loophole.

13) **Fast flux:** is a technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. This sophisticated technique is used to hide the location of criminal servers, complicating the process of tracking them down. The Storm worm is one of the recent malware variants to make use of this technique.

14) **Hacker:** person involved in computer security/insecurity, specialising in the discovery of exploits in systems (for exploitation or prevention), or in obtaining or preventing unauthorised access to systems through skills, tactics and detailed knowledge. Depending of the motivation there are differentiations between black-hat hacker (a malicious or criminal hacker), white-hat hacker (ethical hackers) and grey-hat hackers (ethically ambiguous).

15) **Honeypot**: an individual computer or a network of machines set up to look like a poorly protected system but which records every attempt, successful or otherwise, to compromise it. Often the first hints of a new rash of malicious programs come from the evidence collected by honeypots. Now cybercriminals are tuning their malware to spot when it has compromised a honeypot and to leave without taking over.

16) **IP Address**: the numerical identifier that every machine attached to the Internet needs to ensure the data it requests returns to the right place. IP is an acronym of Internet Protocol and the technical specification defines how this numerical system works.

17) **Malware**: portmanteau term for all malicious software covers any unwanted program that makes its way on to a computer. Derived from Malicious software.

18) **Peer-to-peer networks (P2P)**: in a P2P network the 'peers' are computer systems that are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client. Once connected to the network, P2P software allows you to search for files on other people's computers. Meanwhile, other users on the network can search for files on your computer, but typically only within a single folder that you have designated to share.

19) **Phishing**: the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. The practice is often done by sending e-mails that look as if they come from a financial institution and that seek to trick people into handing over confidential details. Often they direct people to another website that looks like that of the bank or financial institution the e-mail purports to have come from.

20) **Pharming**: is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent. Pharming has been called 'phishing without a lure'.

21) **Ripper**: vendors on underground servers who conduct fraudulent transactions such as not delivering purchased goods, or deliberately sell invalid or fake credit cards.

22) **Script Kiddie**: unskilled hacker, usually not an expert in computer security, who breaks into computer systems by using pre-packaged automated tools written by others.

23) **Skimming**: is the theft of credit card information used in an otherwise legitimate transaction. Instances of skimming include stealing the information of the magnetic stripe and the pin number from an ATM (automated teller machine), or using a fake point of sale terminal in a commercial establishment (shop, restaurant, petrol station, etc).

24) **Spamming**: is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Increasingly, e-mail spam today is sent via 'zombies', that is, networks of virus- or worm-infected personal computers. Many modern worms install a backdoor allowing the spammer access to the computer and use it for malicious purposes.

25) **Spear phishing**: is an e-mail spoofing fraud attempt that targets a specific organisation, seeking unauthorised access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. In spear-phishing the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

26) **Spyware**: is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer, without the user's informed consent. Spyware programs can collect various types of personal information, such as Internet surfing habit, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, redirecting web browser activity, accessing websites blindly that will cause more harmful viruses, or diverting advertising revenue to a third party. Some are now starting to record mouse movements in a bid to foil the latest security measures.

27) **Trojan**: like the wooden horse of legend this is a type of program or message that looks benign but conceals a malicious payload. Many of the attachments on virus-bearing e-mail messages carry Trojans.

28) **Virus**: is a computer program that can copy itself and infect a computer without permission or knowledge of the user. The term 'virus' is also commonly used, albeit erroneously, to refer to many different types of malware and adware programs. It usually requires action to successfully infect a victim (for example, open an attachment in an infected e-mail).

29) **Vishing**: is the criminal practice of using social engineering over the telephone, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information for the purpose of financial reward. The term is a combination of 'voice' and phishing.

30) **Whitehat hacker**: a hacker that uses his or her skills for positive ends and often to thwart malicious hackers. Many whitehat security professionals spend their time looking for and closing the bugs in code that blackhats are keen to exploit.

31) **Worm**: self-propelled malicious program that scours the web seeking new victims – in the past this has been used to distinguish it from a virus that requires user action to compromise a machine. Worms can infect and take over computers without any help, bar lax security, from a victim.

32) **Zombie**: another name for a hijacked computer that is a member of a botnet.

Acknowledgements

Numerous people assisted in the preparation of this report, either as interviewees, workshop attendees, or commentators on earlier drafts. We are grateful to the Computer Crime Unit of the Metropolitan Police Service and other law enforcement agencies, banks and credit card companies and academics that chose not to be identified or singled out for thanks and have not been included in the list below.

Dr. Richard Clayton – Researcher, University of Cambridge Computer Laboratory
Saar Drimer – Researcher, University of Cambridge Computer Laboratory
Michael Hallowes – Detective Chief Superintendent Head of Strategic Operations, National Policing Improvement Agency
Simon Heron – Internet Security Analyst, Network Box Corp (UK) Limited
Dr. Christopher Laing – Senior Lecturer School of Computing Engineering and Information Sciences, Northumbria University
Dr. Brian Moore – Senior Lecturer of Computer Security, University of Coventry
Dr. Steven Murdoch – Researcher, University of Cambridge Computer Laboratory
Duncan Steele – Security Supervisor, Sussex Police
Jill Stevens – consultant on consumer and media affairs and editor of Equality and Diversity Professional
Steve Summerlin – Senior Investigations Manager, Barclays Bank
Phil Taylor – Detective Sergeant, Crime Operations Branch, Hi Tech Crime Unit, Sussex Police
Andrew Tyrer – Leader, Network Security Innovation Platform, Technology Strategy Board
David S Wall – Professor of Criminal Justice and Information Society, Centre for Criminal Justice Studies, School of Law, University of Leeds
Tim Warner – Sales Director and UK Country Manager, Finjan Vital Security
Roy West – Detective Inspector Cheque and Credit Card Unit, City of London Police
Dr. Paula Wilcox – Principle Lecturer, Applied Social Science, University of Brighton
Colin Whittaker – Head of Security, APACS, The UK Payments Association