House of Commons
Home Affairs Committee

E-crime

Fifth Report of Session 2013–14

Report, together with formal minutes, oral and written evidence

Additional written evidence is contained in Volume II, available on the Committee website at www.parliament.uk/homeaffairscom

Ordered by the House of Commons to be printed 17 July 2013

HC 70
[Incorporating HC 618, 2012–13]
Published on 30 July 2013
by authority of the House of Commons
London: The Stationery Office Limited
£20.00

Home Affairs Committee

The Home Affairs Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Home Office and its associated public bodies.

Current membership

Rt Hon Keith Vaz MP (*Labour, Leicester East*) (Chair)
Nicola Blackwood MP (*Conservative, Oxford West and Abingdon*)
James Clappison MP (*Conservative, Hertsmere*)
Michael Ellis MP (*Conservative*, *Northampton North*)
Lorraine Fullbrook MP (*Conservative, South Ribble*)
Dr Julian Huppert MP (*Liberal Democrat, Cambridge*)
Steve McCabe MP (*Labour, Birmingham Selly Oak*)
Bridget Phillipson MP (*Labour, Houghton and Sunderland South*)
Mark Reckless MP (*Conservative, Rochester and Strood*)
Chris Ruane MP (Labour, Vale of Clwyd)
Mr David Winnick MP (*Labour, Walsall North*)

The following Member was also a member of the Committee during the Parliament.

Rt Hon Alun Michael MP (*Labour & Co-operative, Cardiff South and Penarth*)
Karl Turner MP (*Labour, Kingston upon Hull East*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the Internet via www.parliament.uk.

Publication

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the Internet at www.parliament.uk/homeaffairscom.

Committee staff

The current staff of the Committee are Tom Healey (Clerk), Robert Cope (Second Clerk), Eleanor Scarnell (Committee Specialist), Andy Boyd (Senior Committee Assistant), Michelle Garratty (Committee Assistant), Iwona Hankin (Committee Support Officer) and Alex Paterson (Select Committee Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Home Affairs Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 3276; the Committee's email address is homeaffcom@parliament.uk.

Contents

Report

Page

Introduction

1. We live in a world where terms like "Cyber crime" no longer belong in the realm of science fiction. Modern devices such as smart phones and tablets have brought the internet not only to our fingertips but to our bedsides, our pockets and to our children. And yet there is strong evidence that access to such technology, with all its opportunities and benefits, can put our businesses and our families at increasing risk of exploitation and internet-based crime (E-crime).

2. Identity theft, industrial espionage, credit card fraud, phishing, child exploitation - criminals use the internet as a means to commit a wide range of crimes. Perpetrators range from lone hackers, activist groups, Nation States sponsoring industrial espionage and organised criminal gangs. Victims include individuals who fall prey to scams and password theft to multinational companies such as, famously Sony. The financial details of 23,000 users of Sony Online Entertainment were stolen when its networks were breached by hackers in March 2011. The cost of the clean-up was reportedly $172m and the events caused a 9 % share price drop.

3. The internet has also been used to great effect by criminals to trade their cyber wares. Investigators have uncovered sophisticated black market operations such as DarkMarket and ShadowCrew who use the internet to trade cloned credit card data and bank account details, hire botnets (infected networks of computers) and deliver hacking tutorials. Although difficulties in establishing precise figures about the rate and the cost of cyber crime are acknowledged there is general agreement on its rapidly growing scale. Norton have calculated its global cost to be $388bn dollars a year in terms of financial losses and time lost. This is significantly more than the combined annual value of $288bn of the global black market trade in heroin, cocaine and marijuana.

4. UK governments have had a centralised approach to cyber crime and wider cyber threats since the launch of the UK's first Cyber Security Strategy in June 2009 and the corresponding National Cyber Security Programme (NCSP) launched in November 2011. In the course of this inquiry we have looked specifically at the Home Office's remit under its much heralded Cyber Security Strategy.

1 What is e-crime?

Defining e-crime

5. Like traditional crime, e-crime can take many shapes and can occur at almost any time or in any place. Criminals use a number of methods, depending on skill-sets and goals. There is a variety of different terminology used when referring to internet-related crimes. The terms 'e-crime' and 'cyber crime' are often used interchangeably but during this inquiry we have recognised that there are variations between organisations in the way these terms are defined. Defining e-crime has shaped the manner in which organisations such as the Police and Serious and Organised Crime Agency (SOCA) understand and respond to the evolving criminal threats presented in the digital ages.

6. Cybercrime is defined by police as the use of any computer network for crime.[1] The Home Office and the SOCA-led Cyber Threat Reduction Board (TRB) use a three-fold categorisation, dividing e-crime into:

a) 'pure' online crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to enable further crime);

b) 'existing' crimes that have been transformed in scale or form by their use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale; and

c) use of the internet to facilitate drug dealing, people smuggling and many other 'traditional' types of crime.

7. The TRB's broad definition recognises the transformational effect of the internet and computer systems in existing crimes. Other organisations include specific offences: the Council of Europe's Cybercrime Treaty uses the term cybercrime to refer to offences ranging from criminal activity against data to content and copyright infringement. The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access with its definition of cybercrime.[2]

8. The European Commission in 2007 proposed a threefold definition similar to TRB's, identifying cyber crime as:

- Traditional forms of crime committed over electronic communication networks and information systems
- The publication of illegal content over electronic media

[1] http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm

[2] United Nations, *Manual on the Prevention and Control of Computer-Related Crime* ,1994

- Crimes unique to electronic networks.

The main offences covered by existing European and national legislation are:

- privacy offences: illegal collection, storage, modification, disclosure or dissemination of personal data;
- content-related offences: the dissemination of pornography, in particular child pornography, racist statements and information inciting violence;
- economic crimes, unauthorised access and sabotage: offences relating to unauthorised access to systems (e.g. hacking, computer sabotage and distribution of viruses, computer espionage, computer forgery, and computer fraud);
- intellectual property offences: violations of the legal protection of computer programs and databases, copyright and related rights.[3]

9. The Association of Chief Police Officers (ACPO) use the following definition of e-crime in its 2009 E-crime Strategy:

> "the use of networked computers or internet technology to commit or facilitate the commission of crime".

10. This broad definition could cover crimes that are facilitated through using the internet as a means of communication. We are concerned that the TRB and the ACPO definitions could be problematic for law enforcement agencies as they risk referring to all crimes whose perpetrators use the internet to organise themselves as 'e-crime'. It is possible that this type of definition could therefore could blur the distinction between crimes carried out using the internet and crimes carried out offline where the internet is used only as an accessory e.g. a drug deal where the dealers communicate via email. Professor Peter Sommer, Visiting Professor at de Montfort University and a Visiting Reader at the Open University explained that "when the term "computer crime" first came into popular usage in the early 1970s the proportion of the population that had access to computers was tiny" and consequently "it was possible to see computer/cyber/e-crime as distinct purely in terms of the demographics of potential offenders".[4] Modern definitions of cyber crime need to recognise that large numbers of crimes are likely to have a "computer" element simply because at least 77% of the population own a PC.[5]

11. We are further concerned that other aspects of e-crime may not be covered within the definitions of cyber crime used by law enforcement agencies. Professor Peter Sommer pointed out that ACPO's definition appeared to exclude "the use of computers to carry out frauds which don't involve networks, the acquisition of illegal material such as child or extreme pornography and the deployment of techniques to generate forged documents".[6]

[3] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm

[4] Ev 101, para 13 (Prof Peter Sommer)

[5] Ofcom, http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK_CMR_2011_FINAL.pdf

[6] Ev 101, para 11 (Prof Peter Sommer)

12. During our inquiry it became clear that the definitions of what constituted e-crime or cyber crime needed frequent revision if organisations wish to attempt to define the rapidly evolving nature of the e-crime threat. However, e-crime is becoming increasingly hard to define as discrete from other crimes because so many criminals now use online devices and generate digital evidence. **Crimes that have been transformed by the internet and those unique to electronic networks should continue to be defined and recorded as e-crime. This will enable the police to develop an appropriate level of sophisticated technical resource to respond to these crimes.**

13. **The ever-increasing incidence of the use of the internet in some form in traditional crimes indicates the futility of special categorisation for such offences. We recommend that more police officers are trained in digital crime detection and equipped with digital forensic skills. These should become standard skills for officers undertaking relevant investigations.**

Recognising the threat of e-crime

14. Since the creation of the World Wide Web in 1991, the internet has become increasingly central to our economy and our society. Internet and other information systems have transformed our working environment, driving economic growth, connecting people and providing new ways to communicate and co-operate.

15. Cyberspace is the term used to describe the internet and other information systems that form an interactive domain made up of digital networks used to store, modify and communicate information. Digital networks underpin the supply of electricity and water to homes, help organise the delivery of food and other goods to shops, act as an essential tool for businesses across the UK and connect our TVs and games consoles to data.

16. We have seen worrying evidence that the growth of cyberspace has also opened up the UK to serious security threats. Constant contact with digital networks is a fact of modern life. The UK Cyber Security Strategy, published by the Cabinet Office in 2011, suggests that this development of technology "will be on the scale of the very biggest shifts in human history, such as the coming of the railways, or even learning to smelt metals." [7] The Strategy goes on to acknowledge that as a country "– we have no choice but to find ways to confront and overcome these threats if the UK is to flourish in an increasingly competitive and globalised world". [8] EMC and RSA, one of the world's major IT infrastructure and service providers, told us that the cybercrime threat was sophisticated, complex, and rapidly evolving. They explained that there was "a thriving criminal ecosystem" that mirrored the legitimate IT market where criminals could "freely buy and sell malicious software and services". EMC and RSA estimated that this rapidly maturing online black market had led to a "tenfold reduction in the cost to access cyber crime tools and services and an increase in the volume and sophistication of attacks".[9]

[7] Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011, Para 2.1-2.3

[8] Cabinet Office, *The UK Cyber Security Strategy, Protecting and promoting the UK in a digital world*, November 2011, Para 2.1-2.3

[9] Ev 86, Executive summary

17. The UK Cyber Security Strategy argues that "the digital architecture on which we now rely was built to be efficient and interoperable". It acknowledges that when internet usage first started to grow in the UK, security was less of a consideration. Yet a growing number of adversaries now use cyberspace to steal, compromise or destroy critical data. The scale of our dependence means that our prosperity, our key infrastructure, our places of work and our homes can all be affected. Art Coviello, Executive Chairman of RSA (the Security Division of EMC2), told us that people overlook the extent to which our increased dependency on digital services has extended opportunities for malicious activity:

> "We have now developed so many web applications, we have so many remote access devices, mobile devices, we have so many points of entry into our enterprise...we have expanded the attack surface and made it literally easier for the attackers to take advantage of us."[10]

18. We discussed the threat of e-crime to the UK with a number of our witnesses. Dr Ian Brown, Associate Director of Oxford University's Cyber Security Centre and Senior Research Fellow at the Oxford Internet Institute, told us that there was "quite a bit of evidence that organised criminal gangs have moved into cybercrime".[11] Commissioner Adrian Leppard, City of London Police, told us that the National Fraud Intelligence Bureau had identified around 1,300 organised crime groups who used fraud as their main means of gaining money. He estimated that a quarter of these groups were using the internet as their "main means" of committing fraud. Work undertaken by the National Fraud Intelligence Bureau had shown that "about 25 countries predominantly target the UK".[12]

19. David Livingstone, Associate Fellow, International Security Research Directorate, Chatham House, explained that the amount of valuable and attractive goods and items that could be found on UK-based IT systems was "probably a relatively rich hunting ground for organised criminal gangs".[13] We were told that the top five countries where organised criminal groups were using e-crime to attack the UK were "mainly eastern European, and Russia".[14] Mike Andrews, National E-Crime Co-ordination Manager for the National Trading Standards E-Crime Centre, told us that e-crime attacks were coming from many places including: other European member states; former members of the eastern bloc; and the far east. He cautioned that it was "very difficult to pinpoint specific locations because it truly is, to use a cliché, a global problem".[15] Art Coviello, Executive Chairman, RSA, cautioned that "one of the problems with any attack is attribution, being able to trace the attack back to its source". He told us that "to point the finger at a particular nation is clearly not the right thing to do" but reasoned "that given the level of sophistication that we see in attacks, it can only be sponsored by nation states".[16]

[10] Q 311

[11] Q 226

[12] Q 64

[13] Q 225

[14] Q 66

[15] Q 135

[16] Q 314

20. We asked our witnesses whether the "war" on e-crime was being fought and won. Commissioner Adrian Leppard, City of London Police, told us that "we are not winning. I do not think we are winning globally, and I think this nature of crime is rising exponentially".[17] Ilias Chantzos, Senior Director, Government Affairs for EMEA and APJ, Symantec reflected that "As the technologies change, the attack surface changes, the techniques that the attackers are going to use change. What is important is that we adjust ourselves and follow that moving target in order to achieve that objective. We will never have 100% security".[18] Art Coviello believed "we can win the war, but we are not winning it yet".[19]

21. David Livingstone, Associate Fellow at the International Security Research Directorate, Chatham House, told us that the "war on cyber crime" was very serious and "getting worse".[20] However, GCHQ's published earlier this year reported that a staggering 80% of cyber attacks could be stopped through basic information risk management.[21] Iain Lobban, Director GCHQ, had previously outlined how cyber crime is not just a national security or defence issue but is something which goes to the heart of our economic well-being and national interest. He stated that "good Information Assurance practice will solve 80% of Government's Cyber Security vulnerabilities. By this we mean observing basic network security disciplines like keeping patches up to date. That, combined with the necessary attention to personnel security and the 'insider' threat, will offer substantial protection for each individual network".[22] However David Livingstone was concerned that whilst such attacks could be prevented by "getting the basics right" the public were generally unaware of what "those basics might be".[23]

22. **It is of great concern that the majority of cyber crime could be prevented by better awareness by the user. Whilst the sophisticated threats will remain, we must do more to protect our information online. The Government and the private sector both have a strong incentive to educate users and maintain awareness of cyber crime. We recommend that, through its various channels, all organisations, businesses and schools must provide users with appropriate information and risk management training.**

23. **We regard as very serious indeed the words of the most senior policeman in the country on online fraud, DAC Leppard of City of London Police who told the Committee that we are not winning the war on E-crime.**

24. **DAC Leppard told us that a quarter of the 800 specialist internet crime officers could be axed as spending is cut. We agree with him that this is a very worrying trend.**

[17] Q 62

[18] Q 311

[19] Q 311

[20] Q 222

[21] GCHQ, *Countering the cyber threat to business*, Spring 2013

[22] Iain Lobban, Director GCHQ, International Institute for Strategic Studies 12 October 2010, www.gchq.gov.uk/Press/Pages/IISS-CyberSpeech.aspx

[23] Q 236

At a time when fraud and e-crime is going up, the capability of the country to address it is going down.

25. **Ministers have acknowledged the increasing threat of E-crime but it is clear that sufficient funding and resources have not been allocated to the law enforcement responsible for tackling it. Professor Ross Anderson told us that "we should be putting more of the cyber budget into policing and less of it into the intelligence sphere, into cyber war."[24] We also note as a principle, that if personal data is held in any database, no matter how secure, there is a risk of it being accessed inappropriately, either through human error or malice.[25] The only way to ensure data does not leak is not to collect it.**

[24] Q 121

[25] Qq 131–132 [Professor Ross Anderson & Professor Peter Sommer]

2 The Cyber Security Strategy

The current strategy

26. The threat to national security from cyber attacks is real and growing. In October 2010, the National Security Strategy identified the cyber threat to the UK, which includes cyber crime, as a Tier One threat. This is a higher threat category than the threat of nuclear attack, but has received less attention and expenditure. That is to say, a threat of the highest priority for UK national security, taking account of both likelihood of cyber attacks and the impact they could have. This assessment brought hostile attacks upon UK cyber space by other states and large scale cyber crime alongside such major threats as international terrorism and international military crisis.[26]

27. Terrorists, rogue states and cyber criminals are among those targeting computer systems in the UK. The Coalition Government's approach to tackling e-crime has been focused on the revised Cyber Security Strategy released in November 2011, which set out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by "building a more trusted and resilient digital environment".[27] The Cyber Security Strategy is an integral part of the National Cyber Security Programme (NCSP) launched in 2010.

28. The NCSP includes:

i. Creating a new cyber crime capability as part of the National Crime Agency
ii. Mainstreaming cyber training throughout the police
iii. Encouraging the use of 'cyber specials' by police forces
iv. Promoting international cooperation and shared understanding of cyber crime
v. Creating a single reporting system for individuals and small businesses to report cyber crime
vi. Ensuring existing legislation is fit for purpose and used to optimum effect
vii. Taking action to tackle hate crime on the internet
viii. Reviewing existing legislation to ensure it remains relevant and effective
ix. Encouraging the courts to use existing powers to impose appropriate sanctions for online offences.

29. Dr Ian Brown, Associate Director of Oxford University's Cyber Security Centre and Senior Research Fellow at the Oxford Internet Institute, told us that winning the war on cyber crime required a broad spectrum response from a number of areas of government. He believed that the Government was working along "the right lines in developing law enforcement". Other witnesses stressed the importance of Government efforts to persuade other countries to take similar action.[28]

[26] Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, CM 7953, November 2010, pg 27

[27] Ev 61, para 16

[28] Q 224

30. However RSA, an American computer and network security company, told us that its experience of dealing with both the public and private sectors suggested that, whilst recent policy initiatives such as last year's National Cyber Security Strategy have advanced the Government's understanding of the cyber threat and how best to respond to it, the private sector remained ahead in terms of understanding its scale and maturity, and implementing appropriate measures to deliver greater security.[29] **We note the increasing threat posed by state industrial espionage, and international e-crime committed for political purposes, such as the purported attacks on the Guardian from Syria and attacks from China on the US media. The Government must not underestimate the danger such attacks pose to our infrastructure and take firm action with offending countries to cease their activities, using international forums to raise these issues.**

31. **We recommend the establishment of a dedicated espionage response team that British companies, media, and institutions can immediately contact to report an attack and who can also provide training in order to counter attacks.**

Measuring e-crime

Why does it matter?

32. The Government has committed £650million to the NCSP to improve the nation's cyber capabilities in order to help protect "the UK's national security, its citizens and our growing economy in cyber space".[30] As the Government strives to reduce overall expenditure, it is of note that this significant resource is being directed against online threats. Witnesses told us that this funding has gone primarily to the intelligence agencies.

33. It is difficult for us to test policy-makers' and enforcement agencies' understanding of the level of threat posed by cyber criminals or where those threats arise in a public environment without compromising their effectiveness. Our witnesses however suggested that, while the potential threat to national security from cyber attack is reasonable well understood, there is a very poor grasp of the persistently high threat of large volume, low level crime online.

34. Whilst security services receive the lion's share of NCSP funding some witnesses have argued that the funding would be better used "locking up more villains".[31] Professor Ross Anderson told us that the NCSP's budget should go to law enforcement and "less of it into the intelligence sphere", as the threat is primarily from a small number of prolific criminal gangs.[32] He explained that the Government had made a "very welcome increase of £640 million in the cyber security budget two years ago, but 59% of it went to GCHQ and only a few million to the police."[33]

[29] Ev 87, para 14

[30] Ev 61, para 16

[31] Q 121

[32] Q 121

[33] Q 121

Concern over UK government measurements

35. The Government's accepted measure on the cost of e-crime to the UK economy is the one produced by the Cabinet Office in conjunction with Detica. A number of our witnesses expressed scepticism regarding this cost estimated of £27bn. Professor Ross Anderson told us that the Detica report had met with 'widespread scorn'.[34]

[34] Ev 21

Title	Author	Date	Methodology	Main conclusions and recommendations	Critical response
The Cost of Cyber Crime	Detica / Cabinet Office	2011	Developed a causal model relating cyber crime types to their impact on the economy Assessed cost in terms of impact on citizens, business and government No detailed workings or assumptions listed, only that cyber crime types were mapped to a 'number of broad categories of economic impact which are generally consistent with the types of parameters used in macro-economic models of the UK'[35] Magnitude calculated using three point estimate (best, most likely and worst case scenarios)	Cost of cyber crime to the UK estimated to be £27bn £3.1bn - cost to citizens 2.2bn – cost to government £21bn – cost to business Cost of cyber crime is 'significant and growing' Business suffers the highest costs as a result of IP theft and industrial espionage Cyber crime reporting is inhibited by fear of reputational damage, the lack of a clear reporting mechanism and the perception that nothing can be done even if crimes are reported Government should start an online forum for UK business to give authoritative and interactive advice on best practice in protection from cyber crime. A central online reporting mechanism could also be located here.	The report has been heavily criticised for not listing the assumptions or definitions used in the modelling more clearly. E.g. how is 'most-likely' scenario defined and on what evidential basis has it been termed the 'most likely'? The methodology used appears to have given rise to some potentially anomalous findings. For example the cost of IP theft to the not- for- profit sector is listed as being £800m but as £400m to the Aerospace and Defence sector. Critics have pointed out that industrial espionage is not a criminal offence in the UK.[36] The report has omitted malware and online child pornography from its estimate.[37] Some witnesses believe the report is indicative of a poor understanding of the scale of e-crime. They see policy as being driven by GCHQ and major cyber security suppliers to increase spend in this area.[38]

[35] Detica, *The Cost of Cyber crime to the UK*, 2011, p5

[36] Ev 102 [Peter Sommer]

[37] Ibid.

[38] Ev 76 [Foundation for Information Policy Research]

36. Professor Peter Sommer told us that the report on the cost of cyber crime produced by Detica, lacked credibility as it excluded "any reference to children, any reference to the effects of malware, but included industrial espionage, which happens not to be a crime in this country". He was also concerned about how precise figures on an industry-by-industry basis of the amount of losses incurred as a result of industrial espionage were generated.[39]

37. Following the controversy prompted by the findings in the Cabinet Office/Detica report, Sir Mark Welland, the Chief Scientific Office at the Ministry of Defence, commissioned further analysis to "unbundle things into direct and indirect costs". [40] Professor Ross Anderson told us that this research resulted in figures which found more credibility with independent experts and within the security and IT communities. [41] Nevertheless it appears that the Home Office at least still relies on the Cabinet Office/Detica figures.

38. **We understand that any measure of crime will always be subject to challenge and e-crime even more so. However we are puzzled that the Government continues to use highly controversial figures, in which independent experts or indeed other government departments such as the Ministry of Defence have little confidence, as its basis for policy-making.**

39. **Improving the way in which e-crime is reported and recorded is key to improving Parliament's and the public's understanding of it. It is important that policy makers have an up to date and accurate estimate of the threats from e-crime. We therefore recommend that the Government publicly distances itself from the £27bn estimate of the annual cost of e-crime to the UK economy.**

40. **We recommend that the Government commission a working group of experts, drawing on existing good practice already developed by academia and industry, to produce annual figures which show the incidence of e-crime and any observable trends. This group should include representatives from the cyber security industry and independent experts to ensure the figures are robust.**

Trends in e-crime

41. The UK's crime statistics demonstrate that the incidence of e-crime is high and increasing. Surveys, such as the British Crime Survey, demonstrate that individual cyber crime victimization is significantly higher than for 'conventional' crime forms. Victimization rates for online credit card fraud, identity theft, responding to a phishing [42] attempt, and experiencing unauthorized access to an email account, vary between 1 and 17 per cent of the online population for 21 countries across the world, compared with typical

[39] Ev 101

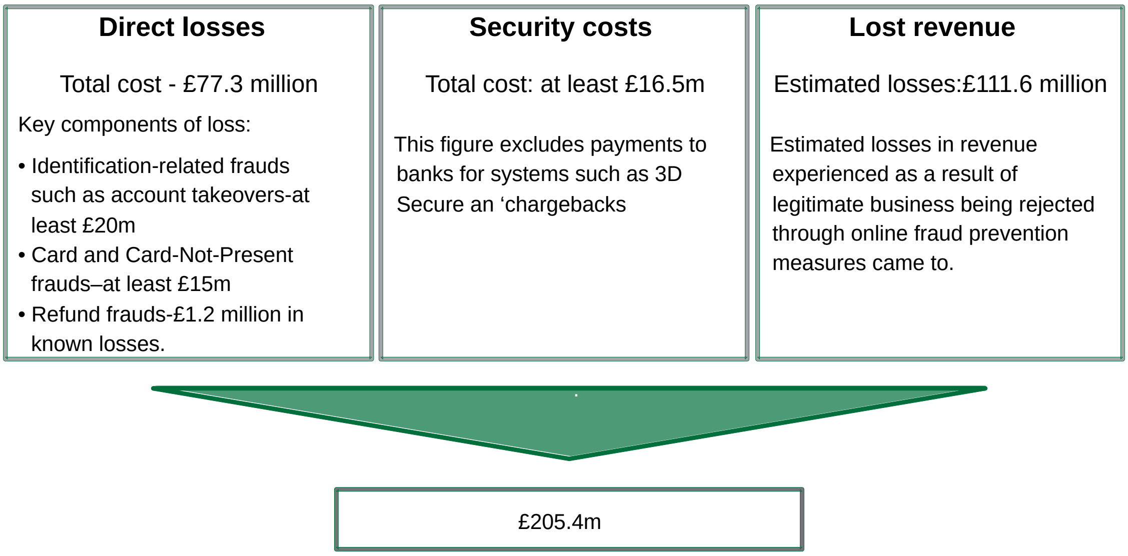
[40] Q 120

[41] Ross Anderson and Foundation for Information Policy Research, *Measuring the Cost of Cybercrime*

[42] See glossary

burglary, robbery and car theft rates of under 5 per cent for these same countries.[43] We note that many victims of e-crime will not be aware that they are victims.

42. The British Retail Consortium (BRC) is the lead trade association for the retail sector representing the whole range of retailers, from small independent stores through to the large multinational companies such as Tesco and Marks and Spencer. The BRC's Retail Crime Survey for 2011-2012 found that the total cost of e-crime to the retail sector was £205.4 million in 2011-12. The diagram below shows that this cost is made up from direct losses, spending on security and lost revenue.



Direct losses

Total cost - £77.3 million

Key components of loss:

- Identification-related frauds such as account takeovers-at least £20m
- Card and Card-Not-Present frauds–at least £15m
- Refund frauds-£1.2 million in known losses.

Security costs

Total cost: at least £16.5m

This figure excludes payments to banks for systems such as 3D Secure an 'chargebacks

Lost revenue

Estimated losses:£111.6 million

Estimated losses in revenue experienced as a result of legitimate business being rejected through online fraud prevention measures came to.

£205.4m

43. Evidence from RSA and Symantec also attest to an increase in the threat from e-crime. The RSA's Anti Fraud Command Centre (AFCC) combines counter-intelligence, threat monitoring, and threat analysis capabilities to neutralise attempts by cyber criminals to steal money and information. In the first seven years of its operation, the AFCC shut down more than 500,000 cyber attacks. The first six months of 2012 saw an increase in attacks with the AFCC shutting down 150,000 attacks, at a rate of 1,000 attacks per day. In June and July 2012 RSA dealt with 250,000 attacks, on average about one per minute. Based on this experience RSA has told us that " the cyber threat is increasingly significant and it is now crucial for all sectors to recognise the dangers involved and respond".[44]

44. Symantec reported similar experiences. It told us it undertakes an annual global study of e-crime threats and trends in e-crime. Based on the data used for its 2011 report it told us that in 2011 Symantec blocked more than 5.5 billion malicious attacks, an increase of more than 81% from the previous year. Symantec's report identified the following trends:

- The number of unique malware identified by Symantec increased by 41% on the previous year;
- The number of web attacks blocked per day increased by 36% on the previous year;

[43] UNODC Comprehensive Study on Cybercrime

[44] Ev 88, para 17

- An increasingly high volumes of malware[45] attacks along with an increase in sophisticated targeted attacks, whe re the user may not know they are being attacked due to the ability of the attacker to slip under the radar and evade detection;
- A rise in advanced persis tent threats and attacks on the infrastructure of the internet itself;
- An increase in the number of data breaches of individuals and business information with more than 232.4 millio n identities worldwide exposed overall during 2011; and
- A reduction in the overall level of spam (a popular vehicle for conducting cyber crime) from 85.5% of all email in 2010 to 75.1% in 2011. Symantec says this reduction is largely seen as being due to law enforcement action which shut down Rustock, a massive worldwide botnet,[46] responsible for sending out large amounts of spam.

45. The latest Norton Cybercrime Report published in September 2012 with findings based on a survey of more than 13,000 adults across 24 countries, reported that there were an estimated 556 million victims of cyber crime each year. This is more than the entire population of the European Union. In the UK, Norton estimated that more than 12.5 million people had fallen victim to cybercrime within the past twelve months. The cost of these cyber crimes to the UK was a massive £1.8 billion with an average cost of £144 per cybercrime victim -bearing in mind how many people are not aware of the crimes, this is probably an underestimate.[47]

[45] Malware is malicious computer code that can be classified into four main threat types: viruses, backdoors, worms and Trojans.

[46] See glossary

[47] Norton Cybercrime Report, September 2012

3 Law enforcement and legislation

New national law enforcement landscape

46. RSA told us that it was necessary "for the government to start taking a more proactive approach to tackling e-crime, rather than relying on the largely reactive structures currently in place". They noted that one "notable exception" was the highly successful Child Exploitation and Online Protection Centre which actively sought to prevent the sexual abuse of children and catch those involved perpetrating these crimes. RSA suggest that the Government consider expanding "this pre-emptive policing framework to confront other forms of cyber crime head on".[48]

47. In response to such criticism, the Government has proposed changes to the national law enforcement e-crime landscape. The National Crime Agency (NCA) will be established by the end of 2013 under provisions granted by the Crime and Courts Act 2013 and will sit the centre of the reformed law enforcement landscape.

48. As part of the NCA, it is proposed to establish a National Cyber Crime Unit (NCCU), to focus on tackling two types of cyber crime:

a) crimes that can only be committed by using computers and the internet, and that occur where a digital system is the target as well as the means of attack. This includes attacks on computer systems to cause disruption (for example Distributed Denial of Service (DDoS) attacks[49]), and the stealing of data over a network often to enable further crime (for example through the spread of viruses and other malware, or computer and network intrusions (hacking).

b) "existing" or traditional crimes that have been transformed in scale or form by the use of the internet, such as fraud or the sharing of indecent images of children. The growth of the internet has opened up a new (often global) market for these crimes, which allows for a degree of anonymity, operation on an industrial scale, and has created new opportunities for organised criminal groups to finance their activities.

49. The Home Office told us that by focusing on these two categories of cyber crime the NCCU will use its resources and skills to tackle the most sophisticated areas of cyber crime, whilst supporting the NCA and wider law enforcement in taking responsibility for tackling cyber-enabled crime. This principle of supporting general law enforcement to assume responsibility for tackling cyber enabled crime, rather than looking to a specialist cyber unit to lead, will underpin the work of the NCCU. It will bring together the national law enforcement response to cyber crime under one roof. This single capability to work closely

[48] Ev 88, para 21

[49] See glossary

with other partners, such as GCHQ, is intended to strengthen the UK's overall resilience and incident response to cyber threats.[50]

50. The Government intends that the third type of cyber crime, that of crimes that are facilitated by the internet, will be tackled by usual policing. The Police are mainstreaming cyber awareness, capacity and capabilities throughout their service.[51]

51. The Home Office argues that the National Cyber Crime Unit will deliver a range of benefits to the current law enforcement response to cyber-enabled crime, including:

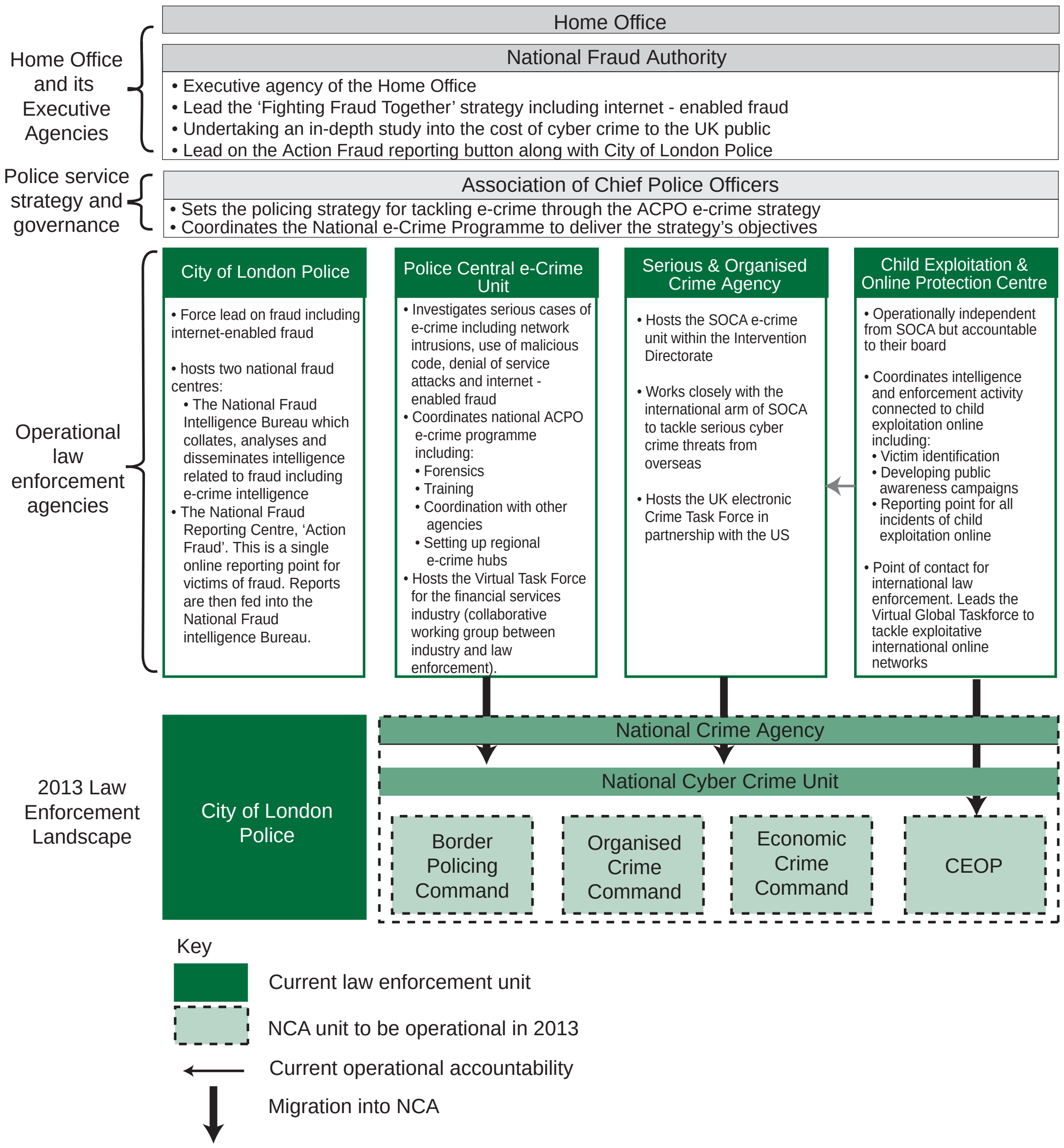
- A single, high-profile law enforcement lead dedicated to combating organised cyber criminals;
- A more targeted focus on the most serious incidents of cyber crime, removing the criminals who facilitate cyber-enabled crime further downstream;
- A stronger, more cohesive response to the most serious cyber-enabled crime;
- Dedicated resources to drive a step-change in cyber capabilities across law enforcement, police service and wider partners;
- Stronger partnerships at all levels, including delivery of a single point of contact for rapid response to dynamic threats and closer engagement with industry and academia;
- Closer joint working with the Security and Intelligence Agencies through improved ICT connectivity and intelligence sharing.[52]

The diagram below illustrates the key changes envisaged to the law enforcement under the NCSP.

[50] Ev 63, para 30

[51] Ev 62, para 29

[52] Ev 63, para 31


Home Office and its Executive Agencies
Police service strategy and governance
Operational law enforcement agencies
2013 Law Enforcement Landscape
Home Office
National Fraud Authority
Association of Chief Police Officers
City of London Police
Police Central e-Crime Unit
Serious & Organised Crime Agency
Child Exploitation & Online Protection Centre
National Crime Agency
National Cyber Crime Unit
City of London Police
Border Policing Command
Organised Crime Command
Economic Crime Command
CEOP
Key

National Fraud Authority

- Executive agency of the Home Office
- Lead the 'Fighting Fraud Together' strategy including internet - enabled fraud
- Undertaking an in-depth study into the cost of cyber crime to the UK public
- Lead on the Action Fraud reporting button along with City of London Police

Association of Chief Police Officers

- Sets the policing strategy for tackling e-crime through the ACPO e-crime strategy
- Coordinates the National e-Crime Programme to deliver the strategy's objectives

City of London Police

- Force lead on fraud including internet-enabled fraud
- hosts two national fraud centres:
  - The National Fraud Intelligence Bureau which collates, analyses and disseminates intelligence related to fraud including e-crime intelligence
- The National Fraud Reporting Centre, 'Action Fraud'. This is a single online reporting point for victims of fraud. Reports are then fed into the National Fraud intelligence Bureau.

Police Central e-Crime Unit

- Investigates serious cases of e-crime including network intrusions, use of malicious code, denial of service attacks and internet - enabled fraud
- Coordinates national ACPO e-crime programme including:
  - Forensics
  - Training
  - Coordination with other agencies
  - Setting up regional e-crime hubs
- Hosts the Virtual Task Force for the financial services industry (collaborative working group between industry and law enforcement).

Serious & Organised Crime Agency

- Hosts the SOCA e-crime unit within the Intervention Directorate
- Works closely with the international arm of SOCA to tackle serious cyber crime threats from overseas
- Hosts the UK electronic Crime Task Force in partnership with the US

Child Exploitation & Online Protection Centre

- Operationally independent from SOCA but accountable to their board
- Coordinates intelligence and enforcement activity connected to child exploitation online including:
  - Victim identification
  - Developing public awareness campaigns
  - Reporting point for all incidents of child exploitation online
- Point of contact for international law enforcement. Leads the Virtual Global Taskforce to tackle exploitative international online networks

🟩 Current law enforcement unit

▨ NCA unit to be operational in 2013

← Current operational accountability

↓ Migration into NCA

52. In its evidence to our inquiry, RSA cautioned that the Government that:

> "must ensure that NCA's remit, and the boundaries and inter-relationships with other agencies involved with e-rime, are well understood by all. Furthermore, it is imperative for the agencies currently involved in the response to e-crime to continue functioning at their optimum level throughout the transition process to prevent criminals taking advantage of any potential lapses in effectiveness or increased vulnerability".[53]

53. **We welcome the steps being taken by Government to bring together different cyber crime units into the NCA to form a single National Cyber Crime Unit. This rationalises the current confusing plethora of different agencies and police organisations involved**

[53] Ev 88, para 22

and should enable a more co-ordinated approach, strong strategic leadership and development of the elite level of skill required to tackle this cyber war.

54. **We were concerned however that the National Fraud Reporting Centre and the National Fraud Intelligence Bureau based in the City of London Police were not being transferred into the NCA. In our view it makes sense to concentrate the national reporting, investigative and intelligence structures for e-crime in one organisation. We were surprised at the decision given the formation of the new economic crime command in the NCA and given we were told that the UK was the main online target of gangs in 25 countries.**

55. **The Committee's report on grooming published earlier this year found that sexually exploited children were still being failed by statutory agencies, and the recent court cases of Mark Bridger and Stuart Hazell have highlighted the role of online indecent images in child abuse. An NSPCC Freedom of Information request revealed that five police forces alone had seized 26 million indecent child images and 2,312 people were arrested for such offences last year. CEOP also estimates there 50,000 indecent child images on Peer 2Peer networks. We are therefore alarmed that CEOP is having its budget cut by 10% over 4 years, its experienced Chief Executive is leaving and it could lose its laser-like focus when merged with the NCA.**

56. **We also note DCS McMurdie's comments that e-crime sentences are too lenient. We were surprised by the fact Anonymous hackers who cost Paypal over £3.5m were given sentences of 7 and 18 months and do not believe they would have received such sentences had they physically robbed a bank of £3.5 million. The DPP should review the sentencing guidance and ensure e-criminals receive the same sentences as if they had stolen that amount of money or data offline.**

Regional and local capability

Regional hubs

57. One of the key aims of the Government's Cyber Security Strategy is to improve the understanding of e-crime and the skills to investigate it across the police service. The Strategy commits the police to:

a) Mainstream cyber awareness, capacity and capabilities throughout its service;

b) Encourage the use of 'cyber specials' to bring in those with the required specialist skills; and

c) Increase law enforcement agency capability on e-crime and develop new training to do so.

58. Police Central e-Crime Unit has delivered three regional e-crime hubs to build on its national capability and improve regional capability and response times. The hubs were

launched in February 2012 and are based in the North West, East Midlands and Yorkshire and Humber.[54]

59. **We welcome the establishment of regional hubs to support and develop local capacity and skills. Mainstreaming e-crime investigative skills throughout the police force is key to improving capacity across the board. We welcome the work currently being undertaken by Police Central e-crime Unit and others in this area.**

60. **However commitments to improve mainstream skill levels have been around for years and practice has not so far matched rhetoric. We hope to see clear evidence that the work promised is being undertaken and clear benchmarks to measure if skills are improving.**

Processing Digital evidence – digital forensics

61. The profusion data and the multiplication of devices upon which it is stored make it impossible for the police to examine all data and devices which may contain information relevant to investigations. The police refer to the process by which they decide what potential digital evidence to seize and examine as triage. Some of our witnesses suggested that insufficient attention was paid to how and by whom such triage was conducted.

62. In her evidence to the Committee, DS McMurdie said that work was being done to train all front line officers in the search and seizure of digital material and that the option of training digital scenes of crime officers was also being considered.[55] Andy Archibald, the Deputy Director of SOCA's Cyber Crime Unit, told us that SOCA were training officers as Digital Forensics Officers.[56]

63. Professor Peter Sommer, who acts as an expert witness in digital forensics, supported the move to improve digital forensics in-house. He reasons that it is vital that the forensic team work with the investigating officer in order to reconstruct events accurately. Both Professor Sommer and Professor Anderson assessed current capacity in the police as patchy. They found pockets of excellence, in SOCA and the Police Central e-crime Unit, but more widely there was still a considerable lack of necessary skills.

64. **We welcome the development of specialist Digital Scenes of Crime and forensic officers and note that the search and seizure of digital material should only be done when it is proportionate.**

International capacity and cooperation: working in partnership and obtaining evidence from overseas

65. The majority of cyber criminals operate outside of the UK's jurisdiction, SOCA told us that this hindered identification and prosecution. Criminal groups were able to base themselves in a number of different jurisdictions and could therefore operate from

[54] More detail on the role of regional hubs can be found in Peter Goodman's evidence from 20 November 2012.

[55] Q 90 [DCS McMurdie]

[56] Q 90 [Andy Archibald]

countries with weak criminal sanctions for online offences. The Police Central e-crime Unit found it difficult to obtain evidence from countries with whom the UK had no established relationship.[57] Andy Archibald, Deputy Director, Cyber and Forensics, Serious Organised Crime Agency, told us that " relationships had to be worked at and worked at hard. We need to identify those countries that have the greatest impact on the UK, and how we can leverage some assistance or some co-operation from them". [58] In order to do this, he explained, placing staff in international partnerships was pivotal:

> We have relationships in a number of areas internationally-with Interpol, with Europol, with the Commonwealth Cyber Initiative-and we have liaison officers in some key locations overseas. In relation to the EU, we have a member of staff with a cyber skill background embedded in the development of the European Cybercrime Centre, which will go live in January. We want to influence the direction and the vision for that unit to ensure it complements the UK approach..[59]

66. In its one year report on the Cyber Security Strategy 2011, the Cabinet Office highlight international cooperation as being crucial to building 'a vibrant and secure cyberspace'. It says the UK has worked towards this by:

- Encouraging wider adoption of the Budapest Convention on cyber crime, putting in place compatible frameworks of law that enable effective cross-border law enforcement and deny safe havens to cyber criminals
- Building a wide network of international partners
- Strengthening relationships with traditional allies and building relationships with a 'broad range' of countries
- Improved international cooperation to tackle cybercrime through legislation and operation work
- Established the Cyber Capacity Building Fund

67. DAC Hewitt argued that the most important tool for getting results internationally was establishing a strong relationship between law enforcement agencies:

> 'primarily from our perspective the Police Central e-Crime Unit, which is the main operational unit that is hosted currently within the Metropolitan Police, has developed very strong relationships with most of the key countries and law enforcement in the key countries with which we work, and the Crown Prosecution Service does likewise with the prosecuting authorities'.[60]

The Cabinet Office's forward plan for the Cyber Security Programme included the objective of building cooperation between the UK and international law enforcement agencies including more joint operations.

[57] Q 99

[58] Q 99

[59] Q 97

[60] Q 368

Obtaining digital evidence from overseas

68. Increasingly, the police require access to digital evidence held outside UK jurisdiction. In evidence to us SOCA and Police Central e-crime Unit described the difficulties associated with established processes for obtaining such evidence. For example, obtaining evidence through Multi- Lateral Assistance Treaties (M LATS) was described as being extremely slow (with it often taking months for them to get the evidence they needed) and resource intensive. Detective Chief Superintendent Charlie McMurdie, Head of the Police Central e-Crime Unit, commented:

> One of the issues around that is the timeliness of the response and the volumes of data that we are looking for, and then the legislation for that country to be able to approach the service provider to get the data on our behalf or for them to progress that.[61]

69. **We were alarmed to hear from police witnesses that they often experienced difficulty in retrieving data from sites based abroad. We hope that such companies will adopt a more constructive attitude going forward and be willing to engage with public authorities. They reap huge financial benefits from the public entrusting them with their data and they should be willing to be open and accountable for the actions they take with it.**

EU Justice and Home Affairs measures

70. Under Protocol 36 of the Lisbon Treaty the UK has the option to opt out of police and criminal justice measures adopted under the Maastricht Treaty, provided it does so before December 2014 when the measures will be adopted under the Lisbon framework, thus giving the Court of Justice of the European Union jurisdiction. The Home Secretary has signalled her intention to opt out of these measures. The option applies to all measures en masse. The UK will then be able, subject to agreement by the EU , to opt back in to any of the measures it decides will be of use.

71. There are at present 133 such measures. They can be divided roughly into the following groups: instruments intended to influence substantive criminal law; instruments intended to influence criminal procedure; instruments relating to police co-operation; and instruments designed to secure mutual recognition.[62] A number of instruments that fall into the last two categories could effect on the UK's ability to tackle e-crime.[63]

72. **The international scope of e-crime provides a strong argument that the UK should focus on increasing cooperation between police forces in other states and making these mechanisms as effective as possible. As the proportion and volume of crime with an online element increases, we expect more police investigations to straddle international**

[61] Q 94

[62] CELS, Opting Out of EU Criminal Law: What is actually involved?, September 2012

[63] One measure in the first category 'Measures intended to influence substantive criminal law' relates to e-crime 'Council Framework Decision 2005/222/JHA of the 25 February 2005 on Attacks against Information Systems'. However this has is likely to soon be replaced by a new Directive and the UK has already opted in to the proposal for it. Council Decision 2000/375/JA to combat child pornography on the internet is also a substantive measure but the UK's domestic law already criminalises child pornography on the internet.

boundaries, and more evidence relating to the offences against the UK and its residents to be located in overseas jurisdictions.

73. **To this end, we cannot understand why the UK has refused to support funding for the new Europol Cybe rCrime Centre C3 whic h facilitates vital cross-Europe information sharing. E-crime does not recognise country borders and it is essential that we have strong international cooperation to ensure offenders are brought to justice and citizens protected. Strengthening our defences and international investigation capacity will save money in the long term and we recommend that the UK supports additional EU funding for the Centre.**

74. **We are deeply concerned that EU partner countries are not doing enough to prevent cyber attacks from criminals within their countries on the UK. We w ill return to this matter in our inquiry into the proposal to opt out of the EU police and criminal justice measures which were adopted before the Treaty of Lisbon entered into force.**

Reporting and recording e-crime

Current UK crime recording practises

75. Currently only violations of the Computer Misuse Act 1990 are recorded as electronic crimes. Crimes that are carried out using the internet defined as offences in other Statutes are recorded as an offence under the substantive legislation.[64] There is no central recording of crime under the method by which it was committed. For example online frauds such as lottery and dating scams are recorded as violations of the Fraud Act 2006 and not as e-crimes. The Home Office told us that it is taking steps to improve the identification of e-crimes within recorded crimes and crime surveys.

76. Some of our witnesses stated tha t even crimes that violate the Computer Misuse Act 1990 are usually recorded according to the criminal's intent. For example, a Denial of Service Attack would probably be recorded as extortion if its perpetrato r was using it to blackmail the website owner. A phishing attack could also be recorded as fraud or money laundering. Witnesses say this is largely due to the Crown Prosecution Service's perception that the Computer Misuse Act 1990 exists to fill in gaps in other forms of legislation.[65]

77. Indeed, some of our wi tnesses also raised concerns regarding the recording and reporting of fraud. The Foundation for Internet Policy Re search said that the previous Government's policy change which saw victims of fraud reporting the crime to their banks in the first place rather than to the police meant that the rate of recorded instances of fraud understates the reality. FIPR points to the British Crime Survey which shows that U K households are twice as likely to be victims of fraud than of traditional acquisitive crime.[66] It added that the 2005 policy change had:

[64] Ev 61 [Home Office]

[65] Ev 102 [Peter Sommer]

[66] Ev 75

> "caused the fraud statistics to go down, but it opened up an even larger gap than is usually the case between the crimes reported through the police, on the one hand, and the crime levels reported through victim surveys on the other. Now, for most practical purposes, official recorded crime is useless in determining the level of fraud"[67]

78. The National Trading Standards Board has also questioned the utility of the current reporting and recording system:

> It is fair to say that the current recording mechanisms probably are not adequate because you tend to find that the illicit activity would get recorded as a general fraud or a consumer protection legislation issue in terms of, for example, a trademarks offence if they were counterfeit goods. They tend to get classified under those areas, but the e-crime element is not necessarily always picked up. Therefore, it is fair to say that there is probably a large-scale under-reporting of e-crime and its true economic impact.[68]

79. The British Retail Consortium says that one of the main problems faced by its members in reporting e-crime was the lack of clarity about case acceptance criteria for reporting online fraud or crime to national agencies. It told us that that its members often spent time preparing detailed reports expecting the relevant agency to accept the case but then found that their case had fallen short of the acceptance criteria and needed to be reported locally.[69]

Action Fraud

80. The Government has made 'Action Fraud', the single national reporting centre for financially motivated online crime. Since August 2011 Action Fraud has had the capability to record the enablers of fraud in fraud reporting. Between its launch in August 2011 and April 2012 49,037 reports of fraud were made to Action Fraud, of which 45% were enabled online. The City of London Police say that the majority of traditional frauds have been eclipsed by fraud with an online element.[70]

Improving recording practises

81. A number of our witnesses recommended the introduction of a new field on crime reporting forms to indicate whether or not there is digital evidence related to the reported crime. This would enable the police to build a clearer picture of where digital evidence was important and to allocate resource accordingly. It would also inform decisions about the amount of resource needed in the field of digital forensics.[71] When we put this to Deputy Associate Commissioner Martin Hewitt, the ACPO lead for e-crime, he acknowledged that more information would enable the police to build a better intelligence picture but he

[67] Q 127

[68] Q 138

[69] Ev 70

[70] Ev 81

[71] Q 116

doubted that victims and the person receiving the report would have the level of knowledge needed to accurately record details about how the crime was carried out.

> "The more information we have the better. Recording the method relies on a level of knowledge within the victim and a level of knowledge within the person who is receiving the report to do that effectively, but I think we are trying to get towards that.... The more information the better, but I don't think necessarily the answer is going to be just having more expansive MO submissions on the crime reports ".[72]

82. **We welcome the online Action Fraud reporting function. We recommend that a clear link to the Action Fraud website is placed on websites where people are likely to experience attempted fraud or visit when they believe they have been a victim of online fraud such as police forces, banks, email providers, trading standards.**

83. **Current recording practises are inadequate to give an accurate picture of the extent to which reported crime is committed over the internet. We recommend the introduction of an additional field on crime reporting forms to indicate whether or not there was digital evidence relating to a crime. This would help the police to understand the extent of the problem they were facing and to make sure they have the appropriate resources in place.**

84. **We are very concerned that there appears to be a 'black hole' where low-level e-crime is committed with impunity. Criminals who defraud victims of a small amount of money are often not reported to or investigated by law enforcement and banks simply reimburse victims. Criminals who commit a high volume of low level fraud can still make huge profits. Banks must be required to report all e-crime fraud to law enforcement and log details of where attacks come from. The perceived untouchable nature of these low- level criminal acts is exemplified by the advert s RSA noted on Facebook advertising 'fraud as a service'.**

[72] Q 380

4 Can web service providers protect our data?

Growth of e-crime on social networks

85. Over half of UK households now use social networking sites. Facebook is the most popular social network in the UK with two thirds of internet users having accounts on the site. Facebook told us that it has 33 million UK users and approximately a billion users worldwide.[73] Twitter estimated that it had 10 million users in the UK, 200 million worldwide.[74] Google+ had 2.5m.[75] Social networking has become the most popular online activity, accounting for 19% of all time spent online worldwide.[76] The popularity of social networks and the vast amount of data they store about individuals is making them a prime target for cyber criminals.

86. During our inquiry we spoke to the providers of the most popular web services in the UK: Facebook, Twitter and Google. We asked them if there had been an increase in the number of attacks on services. Facebook's Simon Milner, Director of Public Policy, told us that there was "consistent evidence" that people were hacking Facebook in the UK and the US.[77] Sinead McSweeney, Director of Public Policy EMEA, Twitter, confirmed that there had been an increase in terms of "advanced, persistent threats from sophisticated and well-resourced individuals with expertise, with resources".[78]

Drivers of e-crime on social networks

87. Sophos reported that social networks were an increasingly popular platform for cyber criminals. It linked the rise in e-crime on social media to the trend in mobile cyber crime as users increasingly accessed social networks through mobile phones: 35% of UK mobile phone users accessed social network sites through their phones in 2010-11.[79] Sophos also reported that 50% of all smartphones were connected to Facebook for 24 hours a day. As well as popularity, Sophos has identified the implied trust between users of social networks as being a key reason for being increasingly targeted by cyber criminals. [80]

88. The Norton 2012 Cyber Crime Report, which surveyed c.13,000 adults across 24 countries, identified the targeting of social networks as one of two key trends in the development of e-crime. The report found that:

[73] Q 169

[74] Q 168

[75] Ofcom, the 2012 Telecommunications Market Report, p263-264

[76] ComScore, Top 10 need to know about social networking and where it's headed, p4

[77] Q 172

[78] Q 171

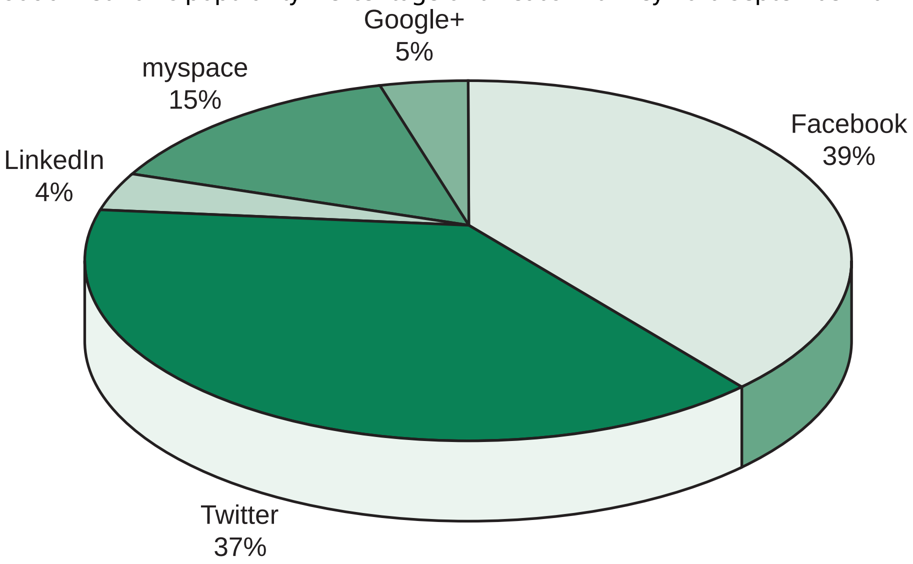
[79] ComScore, Top 10 need to knows about social networking and where it is headed, 2010-11, p20

[80] Sophos, Four Data Threats in a post PC World, p12

- 4 / 10 social network users had been a victim of e-crime on social networks;
- 1/6 social network users reported that someone had hacked into their profile and impersonated them;
- 1/ 10 users had been victims of scams or fake links on social networks.
- 19% of respondents had been notified that their password for a social networking site had been compromised and needed to be changed.[81]

89. Imperva recently analysed the conversation threads on one of the internet's largest hacker forums (it has a membership of 250,000) and a number of smaller forums. It found that social networks were of increasing interest to online hackers. Facebook was the most popular platform discussed, featuring in 39% of conversations. Twitter was a close second, being mentioned in 37% of conversations. Other sites featured can be seen from the chart below. A common request in these discussions was for assistance in hacking into an individual's social network profile, either to spy on them or for revenge.[82]

Social networks popularity. Percentage of threads with keyword September 2011-September 2012 [83]



90. The Police Central e-Crime Unit told us that it saw social networks being used for general and bespoke phishing scams and together information with which to blackmail users.[84]

[81] Norton, 2012 Cyber Crime Report, p13, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[82] Imperva, Hacker Intelligence Initiative, Monthly Trend Report #13, p7

[83] Ibid.

[84] Q 100

Types of e-crime carried out on social networks

Identity theft / phishing on social networks

91. Many types of scams on social networks involve hijacking a user's account by luring them to a webpage with a fake log-in for their account or malware that installs a keylogger (a programme that records key strokes)on their computer. Upon gaining control of the account, the scammer can then contact the user's friends and attempt to scam them by impersonating the user and pretending that they are in trouble and need some money. They can also post messages and links that will compromise their accounts in turn. Accounts may also be hijacked in personally motivated attacks as a means of revenge or to spy on a user's actions.

92. In evidence, RSA explained how users of social media could be providing information unwittingly to criminals: "attackers are increasingly gathering intelligence on their targets, sometimes months in advance of an attack, using social media and other means to understand which individuals possess the assets they want, and crucially how to tailor, or "socially engineer", their attacks to increase their likelihood of success. Indeed cyber attackers prefer using social engineering in this way because in so doing they are able to evade traditional perimeter controls more easily."[85]

Theft of personal information

93. Scammers can steal personal information from social networkers, especially those who do not use privacy settings appropriately (see above) or develop other socially-engineered attacks against the user or their friends. Weaknesses in the design of social networks can help scammer's access personal information. For example the account settings on networks such as Google+ are automatically set to public. Sarah Hunter, Google's Head of Public Policy in the UK, told us that the hijacking of Google accounts was "a significant problem". She said that there was some evidence that phishing emails, as in emails that have been sent to people in an attempt to try to get their passwords out of them, were "increasingly coming from accounts—emails from people they think they know. Of course, they are not from people they know; they are from those accounts that have been hijacked" .[86] Google said it had spent "a lot of money and a lot of time trying to prevent accounts from being hijacked in the first place. We spend hundreds of millions of pounds in keeping our users' data safe".

94. Google appears to have had some success in protecting its users, Sarah Hunter confirmed that over the last two years the number of Google accounts hijacked had decreased by 99.7%. She told us that Google has developed technology that scans account activity and identifies suspicious activity:

> For example, if you have a Gmail account and you signed in from London, and then an hour later signed in from Australia, we would see that as a signal of suspicious activity, and we would ask you a few questions, some security questions; "Are you

[85] Ev 87, para 13

[86] Q 177

> really you?" That is an amazingly effective way to stop hi jacking, and as a result we have significantly reduced the number of hijacked accounts.[87]

95. Facebook has no fo rmal review process for 'apps' developed by th ird parties that are accessible on its platform. Many of these apps require users to give the developer access t o some of their personal account information. Cyber criminals may use apps as another way of evading security checks and stealing personal information.

96. As RSA explained:

> "cyber criminals are out to steal personal information for financial gain. This information can range from an individual's credit card de tails and web or corporate logins, to an orga nisation's highly conf idential plans or data. In deed the value of personal data to a cyber crimin al is much hig her than a cr edit card or bank account number alone. For example, the average selling price of a US credit card on the criminal black market is around $1.50. But when th at card is sold with a full identity profile, the value can be up to ten times greater."[88]

Clickjacking

97. In a practice known as ' clickjacking' malicious code can be hidden beneath legitimate buttons or other clickable cont ent on a website. The content is often given se nsationalist headlines to entice users to clic k on it. Previous examples include: "Lady Gaga found dead in hotel room," and "Japanese tsunami launches whale in to building." Users believe they are clicking on one thing, such as a video or ar ticle but are actually clic king on an invisible button that releases a worm into their computer.[89]

Advance fee / romance scams

98. Cyber criminals may use social network platforms to persuade users to send an advance fee in order to receive a prize or take part in a 'get rich quick' scheme. Scammers have also persuaded users to par t with money by developing an 'online relationship' with individuals.[90] After a while they persuade their victim to send them money on the basis that they are in trouble or want to vi sit the victim in person but can' t afford to do so. This type of fraud is prevalent on dating websites.

Twitter Direct Messages (DMs)

99. One recent s pate of attacks used Twitter Di rect Messages, to tell us ers that they are featured in a YouTube video. Users who click on the link are greeted with what appears to be a video player and a warning message that "An update to YouTube player is needed" but the download is in fact a trojan which will infect the user's computer.

[87] Q 177

[88] Ev 87, para 9

[89] Sophos, Four Data Threats in a post PC World, p12

[90] Sometimes referred to as "catfishing" after the 2010 film of that title

Cyber bullying and Twitter Trolls

100. Cyber bullying and Twitter Trolls are terms that relate to cyber bullying on social media sites. This type of bullying is particularly high amongst young people. Parents have spoken out about their children being bombarded with vicious or sexually explicit taunts from their peers and being pressured to take part in sexual activities, sometimes of a violent nature.[91] There have been several high profile cases of celebrities and public figures becoming victims of 'Twitter Trolls', users who send malicious, offensive and threatening tweets to others. In a recent court case Frank Zimmerman, who sent a message to Louise Mensch threatening her children, was given a 26 week suspended prison sentence.[92] Trolls are not just an issue for Twitter however, Facebook recently launched a campaign in Australia to encourage users to stand up to online bullies. Bullying can and does occur on many other web platforms.

101. **Online services should be 'secure by design' e.g. new account settings should be set by default to private with the user sharing information with friends or publicly only if they actively choose to do so. Users should not be asked to submit personal details that are known to be helpful to fraudsters. For example, users should be discouraged from giving their date of birth.**

102. **We recommend that providers of web services take users through a short explanation when they sign up for an account about how to keep their data secure and how criminals could use certain data against them. Users should not be asked to provide such valuable personal data.**

103. **We are concerned that many users may not grasp the full extent of the data they are sharing with private companies. The interest in and opposition to plans to increase data availability to the Government (e.g. witness the fate of the proposed Data Communication Bill) makes us question whether public are really relaxed about sharing so much data or if they are simply unaware they are doing so.**

104. **We are deeply concerned that it is still too easy for people to access inappropriate online content, particularly indecent images of children, terrorism incitement and sites informing people how to commit online crime. There is no excuse for complacency. We urge those responsible to take stronger action to remove such content. We reiterate our recommendation that the Government should draw up a mandatory code of conduct with internet companies to remove material which breaches acceptable behavioural standards.**

105. **We note those companies that donate to the Internet Watch Foundation, and encourage them to increase their contributions. Additionally, we recommend that the Government should look at setting up a similar organisation focused on reporting and removing online terrorist content.**

[91] Laura Bates, 'Next generation of social media exposing girls to sexual abuse', *The Independent* Website, 13 February, 2013

[92] http://www.guardian.co.uk/uk/2012/jun/11/louise-mensch-troll-sentenced-email

106. **We are concerned to note the Minister's assertion that off the shelf hacking software is increasingly available to untrained criminals and recommend the Government funds a law enforcement team which is focused on disrupting supply.**

Improving software standards

107. Engineering the Future has been outspoken about the need to improve the design of new software to make it more resilient against attack. It says that:

> The capability of seemingly benign attachments, such as pdf files or jpeg pictures to execute malicious code or website attacks ... all result from wholly avoidable mistakes by the developers of the faulty software.
>
> the main source of risk is not, as widely claimed, unsafe behaviour by computer users but, rather, the design flaws and programming errors that make normal, reasonable behaviour unsafe.[93]

108. Engineering the Future says that improving public awareness about online risks will be ineffective if sufficient incentive is not given to software manufacturers to create products that do not expose their customers to such serious risks. It would like to see a timetable announced for introducing a Europe-wide measure of liability on manufacturers and importers of faulty software for the damage that avoidable defects cause.

109. Symantec however has raised doubts, from the point of view of anti-virus software providers, about the extent that software companies can be held responsible for security breaches. It says that since the company cannot control how effectively consumers install and use their products it cannot be liable for a security breach as the fault may lie in the use of the software rather than in its design.

110. It has said that software providers would only accept liability for their products if they could assume a level of control over the way in which they were being used. This, Symantec says, would involve companies using

> 'privacy invasive technology to provide the ability to monitor and control the behaviour and actions of users for example to ensure that the software is being used for only the purpose for which it was supplied or sold.'

111. Symantec says that the legal, privacy and cost issues that this approach would give rise to is unlikely to make it an attractive option for users. It has also said that such an approach would stifle innovation and competition:

> An approach along these lines could not only impact the control users have on their PC's but could also stifle technological innovation and competition in the marketplace by promoting particular business models. A move towards more closed platforms or a situation where one dominant technology provider could dictate what can, or cannot, be installed on its system due to liability concerns may limit

[93] Ev 72

> consumer choices to only sites or online content that are approved by PC providers based on a level of risk.[94]

112. **We recommend that software for key infrastructure be provably secure, by using mathematical approaches to writing code.**

[94] Ev 90

5 Effectiveness of public awareness campaigns

Promoting public awareness

113. Witnesses from the police emphasised the importance of prevention through increasing peoples' awareness of the threats and what they can do to protect themselves.

> "The goal in cyber has to be around prevention activity and developing prevention activity."[95]

Deputy Assistant Commissioner Martin Hewitt, ACPO e-crime lead, told us that we had to get to a point where "as citizens, organisations and businesses, are not, effectively, leaving the windows and the doors open when we leave the office or when we leave the house".[96]

114. Whilst we have heard evidence that a great deal of the responsibility of holding data securely lies with the organisations who hold that information and who develop the software used, it is a fact that criminals often use social engineering methods to target victims. Users are not without responsibility for their own data and can take steps to protect their personal information online. Recent work by Nominet showed that 43% of smartphone and tablet users did not have security measures such as anti-virus software, remote wipe facilities in the case their device is lost or stolen, or the latest version of their operating system installed on their device. The Police e-Crime unit told us that improving awareness about the amount of data that people put in the public domain and what criminals can use it for was key to preventing crime.

> There is a real opportunity, as you have just heard, about public awareness with that. There is freedom of speech, and people put all sorts of information on the internet without realising how vulnerable that makes them. Our information is out there on 500 to 600 different databases at any one time, and the criminal groups run automated programmes harnessing all that data around us, day in, day out, and then they will utilise it to their advantage[97]

Assessing the success of prevention activity in the UK

115. Some of our witnesses have told us about successful public awareness campaigns that have been carried out such as The National Fraud Authority's 'The Devil's in your Details' Facebook campaign. However they also highlighted the difficulties in reaching internet users with information about both staying secure online and also about how to recognise and report fraud if they have been a victim. Adrian Leppard, Commissioner of the City of London Police, told us of the work in prevention going on under the Cyber Security Strategy. However he acknowledged that educating the public was a challenge, noting "We

[95] Q 378

[96] Q 378

[97] Q 101

do have to push that out in better campaigning and much more public messaging about it".[98]

116. In the Commissioner's view, prevention work would be more effective if it:

- Involved stronger partnership with the private sector;
- Used platforms such as television that reached a wide audience;
- Had specific campaigns targeted at different segments of society, particularly vulnerable ones;
- Had more funding from the Government.

The lack of funding for prevention activity was raised as an issue by other witnesses who were concerned that the only prevention work which had specifically been allocated funding by the National Cyber Security Programme-Get Safe Online received £395,000, only 0.06% of the total budget.

117. Other witnesses have argued that prevention has limited utility. Professor Ross Anderson has told us that it put too greater onus on consumers:

> I am not quite as enthusiastic about public education as some other people, because of the simple fact that computers and mobile phones and social networking sites tend to ship with unsafe defaults because it is better for selling advertising.[99]

118. He also argued that since a lot of economic damage is done by a small number of cyber criminals it would be more efficient to arrest and prosecute them.

119. **We recommend that guidance about keeping personal data secure should be incorporated into all online services that request personal data from their users.**

120. **It is as important that children learn about staying safe online as it is that they learn about crossing the road safely. We welcome teaching about online safety and security taking place in schools and initiatives such as 'safer internet week'.**

121. **The children we spoke to believed an important part of learning to stay safe online was being taught to respect others online and not to say things that you wouldn't say to their face and we agree.**

[98] Q 74

[99] Q 130

Annex: Glossary of terms

Apps — (abbreviation for 'application') a piece of software that can run on a computer, a mobile device, or from a web browser.

Bot — a computer that has been compromised to serve the hacker's need without the user's knowledge.

Botnet — a networks of bots which can act together to achieve a collective aim.

Browser — a web browser is a program used to access the World Wide Web

Conversation threads — messages which are grouped together (usually by subject), e.g. on an internet forum or by an email client like outlook or gmail, as a visual aid to the user.

Cookies — small data files generated by a website and saved onto your computer when you first visit the website. Their purpose is to identify you, so that the site can keep track of your movements ; they may also store your personal data or preferences. Some browsers allow users to delete specific cookies or prevent cookies from being created, this allows the user a higher level of privacy but could affect website functionality on their computer as many websites are designed to require cookies to function properly.

- Session cookies — temporary files that are deleted when the browser is closed
- Persistent cookies — files designed to store data for an extended period of time. Each persistent cookie is created with an expiration date, once the expiration date is reached, the cookie is automatically deleted. Persistent cookies are what allow websites to "remember you" for two weeks, one month , or any other amount of time.

Denial of Service (DoS) attack — an attack on a computer system (typically a web server) which aims to make the system unavailable by flooding it with internet traffic so that it becomes overloaded and inoperable.

Distributed Denial of Service (DDoS) attack — as above but carried out by a number of networked computers controlled by one master (a botnet).

Domain Name System (DNS) — The Internet uses the Domain Name System (DNS) to allow computers to identify each other. To connect to the Internet, each computer requires a unique numerical label called an IP address. IP addresses are matched to memorable labels called domain names, stored in a global database. For example, instead of typing the IP address 194.60.38.75, to connect to the computer that hosts the parliamentary website, the domain name www.parliament.uk is used.

Domain names generally follow the format www.xxxxx.yyy, where:

.yyy is the top level domain, which can be a country code such as '.uk' or a generic domain such as '.com' or '.org';

.xxxxx is the second level domain such as '.parliament', '.co' or '.google';

additional subdomains, such as 'www.' can be used to the left.

The DNS is coordinated to ensure addresses and domain names are unique. Due to the number of names and addresses they are stored on specialist computers.

Hosting / website hosting — Housing, serving and maintaining files for websites. A Web Host provides internet access through a system called a server. A Web Hosting company may have many servers to hold many gigabytes of information. This requires a fast connection to the internet and most hosting companies offer fast connections which would be very expensive for businesses to take out for their individual websites.

Internet Protocol (IP) — the method or protocol by which data is sent from one computer to another on the Internet

IP address — see "Domain Name System"

Malware (malicious software) — A catch-all term for software with malicious intent. The uses of malicious software range from placing excessive demand on a computer's resources, to destruction of data or even hardware. In some cases the user is made aware of the presence of the malware, for example when it sends a message to the user or deletes the contents of a hard drive. Recent forms of malware may operate without the user's knowledge, steal financial information such as credit card details, or convert infected computers into an asset for the attacker.

Common types of malware work as follows:

- Viruses infect computers or other electronic devices and are passed on by user activity, for example by opening an email attachment.

- Worms self-propagate using an internet connection to access vulnerabilities on other computers and to install copies of themselves. They are often used as a conduit to grant attackers access to the computer.

- Trojans are malware masquerading as something the user may want to download or install, that may then perform hidden or unexpected actions, such as allowing external access to the computer.

- Spyware transmits information gathered from a computer, such as bank details, back to an attacker. For example 'keylogging' software records anything entered using the keyboard, such as passwords.

Phishing — Sending fraudulent emails to individuals that claim to come from a legitimate source (e.g. internet retailer or bank). The aim of these emails is to persuade the victim to voluntarily disclose sensitive information such as bank account and credit card details that can then be exploited to defraud them.

Root-kit — software to gain and maintain privileged access to computer systems; can be used to conceal other malware;

Trojan / Trojan Horse — Malicious software programmes which are disguised as benign applications such as computer games or antivirus software. Once installed on a system, they can cause data theft and loss, as well as system crashes or slowdowns. Trojans can also be used as launching points for other attacks, such as distributed denial of service (DDoS). Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

URL (Universal resource Locator) — formatted text string used by Web browsers and other software to identify a network resource on the Internet. Network resources are files that can be plain Web pages, other text documents, graphics, or programs. A URL consists of three parts: a network protocol, a host name or address a file or resource location.

Virus — A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it actually cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. Because a virus is spread by human action people will unknowingly continue the spread of a computer virus by sharing infecting files or sending emails with viruses as attachments in the email.

Widgets — a “widget” is an application that sits on top of a Web site and offers users additional interactive features. There are four main types of Widget: (1) a widget engine (such as dashboard apps like Apple’s Mac OS X v10.4, Windows Vista Sidebar, or Yahoo! Widgets), (2) GUI widgets (which are a component of a graphical user interface in which the user interacts), (3) Web widgets (which refer to a third party item that can be embedded in a Web page), and (4) mobile widgets (a third party item that can be embedded in a mobile phone).

Worms — A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver’s address book, and the manifest continues on down the line.

Conclusions and recommendations

C&R Sub heading

1. Crimes that have been transformed by the internet and those unique to electronic networks should continue to be defined and recorded as e-crime. This will enable the police to develop an appropriate level of sophisticated technical resource to respond to these crimes. (Paragraph 12)

2. The ever-increasing incidence of the use of the internet in some form in traditional crimes indicates the futility of special categorisation for such offences. We recommend that more police officers are trained in digital crime detection and equipped with digital forensic skills. These should become standard skills for officers undertaking relevant investigations. (Paragraph 13)

3. It is of great concern that the majority of cyber crime could be prevented by better awareness by the user. Whilst the sophisticated threats will remain, we must do more to protect our information online. The Government and the private sector both have a strong incentive to educate users and maintain awareness of cyber crime. We recommend that, through its various channels, all organisations, businesses and schools must provide users with appropriate information and risk management training. (Paragraph 22)

4. We regard as very serious indeed the words of the most senior policeman in the country on online fraud, DAC Leppard of City of London Police who told the Committee that we are not winning the war on E-crime. (Paragraph 23)

5. DAC Leppard told us that a quarter of the 800 specialist internet crime officers could be axed as spending is cut. We agree with him that this is a very worrying trend. At a time when fraud and e-crime is going up, the capability of the country to address it is going down. (Paragraph 24)

6. Ministers have acknowledged the increasing threat of E-crime but it is clear that sufficient funding and resources have not been allocated to the law enforcement responsible for tackling it. Professor Ross Anderson told us that "we should be putting more of the cyber budget into policing and less of it into the intelligence sphere, into cyber war." We also note as a principle, that if personal data is held in any database, no matter how secure, there is a risk of it being accessed inappropriately, either through human error or malice. The only way to ensure data does not leak is not to collect it. (Paragraph 25)

7. We note the increasing threat posed by state industrial espionage, and international e-crime committed for political purposes, such as the purported attacks on the Guardian from Syria and attacks from China on the US media. The Government must not underestimate the danger such attacks pose to our infrastructure and take firm action with offending countries to cease their activities, using international forums to raise these issues. (Paragraph 30)

8. We recommend the establishment of a dedicated espionage response team that British companies, media, and institutions can immediately contact to report an attack and who can also provide training in order to counter attacks. (Paragraph 31)

9. We understand that any measure of crime will always be subject to challenge and e-crime even more so. However we are puzzled that the Government continues to use highly controversial figures, in which independent experts or indeed other government departments such as the Ministry of Defence have little confidence, as its basis for policy-making. (Paragraph 38)

10. Improving the way in which e-crime is reported and recorded is key to improving Parliament's and the public's understanding of it. It is important that policy makers have an up to date and accurate estimate of the threats from e-crime. We therefore recommend that the Government publicly distances itself from the £27bn estimate of the annual cost of e-crime to the UK economy. (Paragraph 39)

11. We recommend that the Government commission a working group of experts, drawing on existing good practice already developed by academia and industry, to produce annual figures which show the incidence of e-crime and any observable trends. This group should include representatives from the cyber security industry and independent experts to ensure the figures are robust. (Paragraph 40)

12. We welcome the steps being taken by Government to bring together different cyber crime units into the NCA to form a single National Cyber Crime Unit. This rationalises the current confusing plethora of different agencies and police organisations involved and should enable a more co-ordinated approach, strong strategic leadership and development of the elite level of skill required to tackle this cyber war. (Paragraph 53)

13. We were concerned however that the National Fraud Reporting Centre and the National Fraud Intelligence Bureau based in the City of London Police were not being transferred into the NCA. In our view it makes sense to concentrate the national reporting, investigative and intelligence structures for e-crime in one organisation. We were surprised at the decision given the formation of the new economic crime command in the NCA and given we were told that the UK was the main online target of gangs in 25 countries. (Paragraph 54)

14. The Committee's report on grooming published earlier this year found that sexually exploited children were still being failed by statutory agencies, and the recent court cases of Mark Bridger and Stuart Hazell have highlighted the role of online indecent images in child abuse. An NSPCC Freedom of Information request revealed that five police forces alone had seized 26 million indecent child images and 2,312 people were arrested for such offences last year. CEOP also estimates there 50,000 indecent child images on Peer2Peer networks. We are therefore alarmed that CEOP is having its budget cut by 10% over 4 years, its experienced Chief Executive is leaving and it could lose its laser-like focus when merged with the NCA. (Paragraph 55)

15. We also note DCS McMurdie's comments that e-crime sentences are too lenient. We were surprised by the fact Anonymous hackers who cost Paypal over £3.5m were given sentences of 7 and 18 months and do not believe they would have received such sentences had they physically robbed a bank of £3.5 million. The DPP should review the sentencing guidance and ensure e-criminals receive the same sentences as if they had stolen that amount of money or data offline. (Paragraph 56)

16. We welcome the establishment of regional hubs to support and develop local capacity and skills. Mainstreaming e-crime investigative skills throughout the police force is key to improving capacity across the board. We welcome the work currently being undertaken by Police Central e-crime Unit and others in this area. (Paragraph 59)

17. However commitments to improve mainstream skill levels have been around for years and practice has not so far matched rhetoric. We hope to see clear evidence that the work promised is being undertaken and clear benchmarks to measure if skills are improving. (Paragraph 60)

18. We welcome the development of specialist Digital Scenes of Crime and forensic officers and note that the search and seizure of digital material should only be done when it is proportionate. (Paragraph 64)

19. We were alarmed to hear from police witnesses that they often experienced difficulty in retrieving data from sites based abroad. We hope that such companies will adopt a more constructive attitude going forward and be willing to engage with public authorities. They reap huge financial benefits from the public entrusting them with their data and they should be willing to be open and accountable for the actions they take with it. (Paragraph 69)

20. The international scope of e-crime provides a strong argument that the UK should focus on increasing cooperation between police forces in other states and making these mechanisms as effective as possible. As the proportion and volume of crime with an online element increases, we expect more police investigations to straddle international boundaries, and more evidence relating to the offences against the UK and its residents to be located in overseas jurisdictions. (Paragraph 72)

21. To this end, we cannot understand why the UK has refused to support funding for the new Europol CybeRCrime Centre C3 which facilitates vital cross-Europe information sharing. E-crime does not recognise country borders and it is essential that we have strong international cooperation to ensure offenders are brought to justice and citizens protected. Strengthening our defences and international investigation capacity will save money in the long term and we recommend that the UK supports additional EU funding for the Centre. (Paragraph 73)

22. We are deeply concerned that EU partner countries are not doing enough to prevent cyber attacks from criminals within their countries on the UK. We will return to this matter in our inquiry into the proposal to opt out of the EU police and criminal justice measures which were adopted before the Treaty of Lisbon entered into force. (Paragraph 74)

23. We welcome the online Action Fraud reporting function. We recommend that a clear link to the Action Fraud website is placed on websites where people are likely to experience attempted fraud or visit when they believe they have been a victim of online fraud such as police forces, banks, email providers, trading standards. (Paragraph 82)

24. Current recording practises are inadequate to give an accurate picture of the extent to which reported crime is committed over the internet. We recommend the introduction of an additional field on crime reporting forms to indicate whether or not there was digital evidence relating to a crime. This would help the police to understand the extent of the problem they were facing and to make sure they have the appropriate resources in place. (Paragraph 83)

25. We are very concerned that there appears to be a 'black hole' where low-level e-crime is committed with impunity. Criminals who defraud victims of a small amount of money are often not reported to or investigated by law enforcement and banks simply reimburse victims. Criminals who commit a high volume of low level fraud can still make huge profits. Banks must be required to report all e-crime fraud to law enforcement and log details of where attacks come from. The perceived untouchable nature of these low-level criminal acts is exemplified by the adverts RSA noted on Facebook advertising 'fraud as a service'. (Paragraph 84)

26. Online services should be 'secure by design' e.g. new account settings should be set by default to private with the user sharing information with friends or publicly only if they actively choose to do so. Users should not be asked to submit personal details that are known to be helpful to fraudsters. For example, users should be discouraged from giving their date of birth. (Paragraph 101)

27. We recommend that providers of web services take users through a short explanation when they sign up for an account about how to keep their data secure and how criminals could use certain data against them. Users should not be asked to provide such valuable personal data. (Paragraph 102)

28. We are concerned that many users may not grasp the full extent of the data they are sharing with private companies. The interest in and opposition to plans to increase data availability to the Government (e.g. witness the fate of the proposed Data Communication Bill) makes us question whether public are really relaxed about sharing so much data or if they are simply unaware they are doing so. (Paragraph 103)

29. We are deeply concerned that it is still too easy for people to access inappropriate online content, particularly indecent images of children , terrorism incitement and sites informing people how to commit online crime. There is no excuse for complacency. We urge those responsible to take stronger action to remove such content. We reiterate our recommendation that the Government should draw up a mandatory code of conduct with internet companies to remove material which breaches acceptable behavioural standards. (Paragraph 104)

30. We note those companies that donate to the Internet Watch Foundation, and encourage them to increase their contributions. Additionally, we recommend that the Government should look at setting up a similar organisation focused on reporting and removing online terrorist content. (Paragraph 105)

31. We are concerned to note the Minister's assertion that off the shelf hacking software is increasingly available to untrained criminals and recommend the Government funds a law enforcement team which is focused on disrupting supply. (Paragraph 106)

32. We recommend that software for key infrastructure be provably secure, by using mathematical approaches to writing code. (Paragraph 112)

33. We recommend that guidance about keeping personal data secure should be incorporated into all online services that request personal data from their users. (Paragraph 119)

34. It is as important that children learn about staying safe online as it is that they learn about crossing the road safely. We welcome teaching about online safety and security taking place in schools and initiatives such as 'safer internet week'. (Paragraph 120)

35. The children we spoke to believed an important part of learning to stay safe online was being taught to respect others online and not to say things that you wouldn't say to their face and we agree. (Paragraph 121)

Formal Minutes

Wednesday 17 July 2013

Members present:

Keith Vaz, in the Chair

James Clappison	Steve McCabe
Michael Ellis	Mark Reckless
Dr Julian Huppert	Mr David Winnick

Draft Report (*E-crime*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 121 read and agreed to.

Annex agreed to.

Resolved, That the Report be the Fifth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

Written evidence was ordered to be reported to the House for printing with the Report (in addition to that ordered to be reported for publishing on 4 September, 16 October, and 20 and 27 November 2012, and 5 February, 19 and 26 March, and 16 and 23 April 2013).

[Adjourned till Tuesday 3 September at 2.30 p.m.

Witnesses

page

Tuesday 30 October 2012

Peter Davies, ACPO Lead on Child Protection and Abuse Investigation and Missing Children Ev 1

Tuesday 20 November 2012

Deputy Assistant Commissioner Martin Hewitt, ACPO E-Crime Lead, and **Deputy Chief Constable Peter Goodman**, Regional E-crime Lead for East Midlands Ev 8

Tuesday 11 December 2012

Commissioner Adrian Leppard, City of London Police Ev 13

Detective Chief Superintendent Charlie McMurdie, Head of Police Central E-Crime Unit**,** and **Andy Archibald,** Deputy Director, Cyber and Forensics, Serious Organised Crime Agency Ev 17

Professor Peter Sommer and **Professor Ross Anderson** Ev 21

Tuesday 29 January 2013

Tom Ironside, Director of Business and Regulation, British Retail Consortium, and **Mike Andrews,** National E-Crime Co-ordination Manager for the National Trading Standards E-Crime Centre Ev 26

Tuesday 26 February 2013

Sarah Hunter, Head of UK Public Policy, Google, and **Simon Milner,** Director of Policy UK and Ireland, facebook, and **Sinéad McSweeney,** Director of Public Policy EMEA, Twitter Ev 30

Tuesday 16 April 2013

David Livingstone, Associate Fellow, International Security Research Directorate, Chatham House, and **Professor Sadie Creese,** Professor of Cyber Security at the University of Oxford, Director of Oxford University's Cyber Security Centre, and **Dr Ian Brown,** Associate Director of Oxford University's Cyber Security Centre, Senior Research Fellow at the Oxford Internet Institute Ev 41

Anthony Browne, Chief Executive, British Bankers' Association, and **Matthew Allen,** Director, Financial Crime, British Bankers' Association, and **Katy Worobec,** Head of Fraud, Financial Fraud Action UK Ev 46

Tuesday 23 April 2013

Art Coviello, Executive Chairman, RSA, The Security Division of EMC^2, **Professor Jim Norton,** Engineering The Future, and **Ilias Chantzos,** Senior Director, Government Affairs for EMEA and APJ, Symantec Ev 53

List of printed written evidence

List of additional written evidence

(published in Volume II on the Committee's website www.parliament.uk/homeaffairscom)

List of Reports from the Committee during the current Parliament

Session 2013–14

First Report	Police and Crime Commissioners: Register of Interests	HC 69
Second Report	Child sexual exploitation and the response to localised grooming	HC 68-I
Third Report	Leadership and standards in the police	HC 67-I
Fourth Report	The work of the UK Border Agency (Oct-Dec 2012)	HC 486

Session 2012–13

First Report	Effectiveness of the Committee in 2010–12	HC 144
Second Report	Work of the Permanent Secretary (April–Dec 2011)	HC 145
Third Report	Pre-appointment Hearing for Her Majesty's Chief Inspector of Constabulary	HC 183
Fourth Report	Private Investigators	HC 100
Fifth Report	The work of the UK Border Agency (Dec 2011–Mar 2012)	HC 71
Sixth Report	The work of the Border Force	HC 523
Seventh Report	Olympics Security	HC 531
Eighth Report	The work of the UK Border Agency (April–June 2012)	HC 603
Ninth Report	Drugs: Breaking the Cycle	HC 184
Tenth Report	Powers to investigate the Hillsborough disaster: interim Report on the Independent Police Complaints Commission	HC 793
Eleventh Report	Independent Police Complaints Commission	HC 494
Twelfth Report	The draft Anti-social Behaviour Bill: pre-legislative scrutiny	HC 836
Thirteenth Report	Undercover Policing: Interim Report	HC 837
Fourteenth Report	The work of the UK Border Agency (July-Sept 2012)	HC 792

Session 2010–12

First Report	Immigration Cap	HC 361
Second Report	Policing: Police and Crime Commissioners	HC 511
Third Report	Firearms Control	HC 447
Fourth Report	The work of the UK Border Agency	HC 587
Fifth Report	Police use of Tasers	HC 646
Sixth Report	Police Finances	HC 695
Seventh Report	Student Visas	HC 773
Eighth Report	Forced marriage	HC 880
Ninth Report	The work of the UK Border Agency (November 2010-March 2011)	HC 929
Tenth Report	Implications for the Justice and Home Affairs area of	HC 789

	the accession of Turkey to the European Union	
Eleventh Report	Student Visas – follow up	HC 1445
Twelfth Report	Home Office – Work of the Permanent Secretary	HC 928
Thirteenth Report	Unauthorised tapping into or hacking of mobile communications	HC 907
Fourteenth Report	New Landscape of Policing	HC 939
Fifteenth Report	The work of the UK Border Agency (April-July 2011)	HC 1497
Sixteenth Report	Policing large scale disorder	HC 1456
Seventeenth Report	UK Border Controls	HC 1647
Eighteenth Report	Rules governing enforced removals from the UK	HC 563
Nineteenth Report	Roots of violent radicalisation	HC 1446
Twentieth Report	Extradition	HC 644
Twenty-first Report	Work of the UK Border Agency (August-Dec 2011)	HC 1722

Oral evidence

Taken before the Home Affairs Select Committee

on Tuesday 30 October 2012

Members present:

Keith Vaz (Chair)

Nicola Blackwood	Bridget Phillipson
Dr Julian Huppert	Mark Reckless
Steve McCabe	Mr David Winnick

Examination of Witness

Witness: **Peter Davies**, ACPO lead on Child Protection and Abuse Investigation and Missing Children, gave evidence.

Q1 Chair: Mr Davies, good afternoon. You are in demand before Select Committees.
Peter Davies: Indeed.
Chair: I have to tell you that when Jim Gamble went and we heard that CEOP was going to be part of the NCA we were very worried that you might lose your profile, but you now find yourself centre stage as far as these very serious matters are concerned. Could we deal first with Operation Yewtree and the Savile allegations?
Peter Davies: Of course.

Q2 Chair: How are you involved in respect of these allegations? Are you leading an investigation? Are you providing advice to those who are investigating?
Peter Davies: Thank you for the opportunity. Let me explain. In addition to being Chief Executive of CEOP, I am the lead for ACPO—the Association of Chief Police Officers—on child protection, child abuse investigation and missing children. It is in that capacity that I have most involvement with the Jimmy Savile case. Prior to the broadcast of the Exposure programme a few weeks ago, it became very clear from the media that a number of people were coming forward making disclosures, primarily against Jimmy Savile, of abuse that had happened some time ago. At that point there was no way of knowing where the majority, or a substantial chunk of those offences, might have taken place, so we put a process in place, supported by the Metropolitan police, to make sure that there was support for any victims who wanted to disclose through contacting helplines, but also so that we could gather all the data and get the most comprehensive picture possible.

Q3 Chair: You fit in where? You are obviously not running Yewtree; Yewtree is being run by the Met.
Peter Davies: I was just going to come to that. The day after the broadcast, it became clear that at least one of the centres of activity had been London and the Metropolitan police stepped up and volunteered to take on the inquiry. At that point I stepped back. The inquiry, the gathering of data and the commissioning of any investigations following that are in the hands of the Metropolitan police, led by Commander Peter Spindler. Where I retain an interest on behalf of ACPO is that the circumstances around Operation Yewtree may well raise questions that might affect public confidence in policing or provoke questions we should ask of ourselves, because we are very much in the business of making sure that such a series of events could not possibly happen again.
Chair: Indeed.
Peter Davies: I still have an interest in the police service identifying what lessons may be learnt, learning them and acting upon that learning.

Q4 Chair: Very helpful. When you last came before us you rated the public sector's ability to protect children from child exploitation as being five out of 10. Knowing what you now know and looking at the whole situation since you have been director, would you improve on that score for the public sector or do you think it is worse than you suspected?
Peter Davies: I gave two scores: one for effort, one for attainment.
Chair: Yes you did.
Peter Davies: I think both scores would have gone up in the intervening period. There is evidence, for example, from Barnardo's, who published a report in April this year that showed that a significant proportion of Local Safeguarding Children Boards—who very much have the best opportunity to impact on this—had committed to far greater activity than was apparent to us when we did our thematic assessment the previous year. I have contacts both through ACPO and through CEOP with a number of police forces and with institutions such as the National Working Group, led by Sheila Taylor MBE.
It seems extremely clear that practitioners are embracing the need to learn more, improve their processes, invest resources and knowledge in dealing more effectively with group-related child sexual exploitation. Effort has moved up, attainment has moved up, because more forces are delivering investigations, and I know of a number of proactive investigations yet to see the light of day that are taking place around the country. Both scores have improved. *[Interruption.]* I apologise, I am trying to talk over the bell.
Chair: No, we should apologise to you. You are giving us some very interesting information. I am not sure whether that is a vote or they are just telling us they are closing. Let us go on. You paint a better

picture, but yesterday you were quite critical, were you not? You said you were sad and angry that until recently some frontline professionals had struggled to grasp the complex nature of sexual exploitation.

Peter Davies: The issue is how far I cast my eyes back.

Chair: Mr Davies, I apologise. I was relying on the information of Mr Winnick who is very experienced and distinguished, because I too saw Remaining Orders of the Day. However, he was wrong. We are going to suspend the Committee for the vote, but I know you are in difficulties.

Peter Davies: I might have difficulties because of another Committee.

Chair: I assure that the next Committee is also going to be voting, so they will all be ten minutes late.

Peter Davies: Thank you. I will be here.

Chair: Okay, so I am going to suspend the Committee for 10 minutes.

Sitting suspended for a Division in the House.

On resuming—

Q5 Chair: To repeat my question, in case people have forgotten, only yesterday you said you were sad and angry that until recently some frontline professionals had struggled to grasp the complex nature of sexual exploitation. You launched a very helpful video, which is now on YouTube, but does that not show that people are just not trained to deal with this very important issue, even now in 21st-century Britain?

Peter Davies: Yes, could I just separate a couple of things? Thank you for acknowledging the training video. What I was referring to there were some examples when it seemed very clear that people had not taken steps to identify a child at risk and done the right thing by them. I think for anybody who has spent their whole working life trying to protect the public, “sad” is not quite adequate for how you feel about that, because that is not what any of us joined the police service for. My role at the moment is not to say everything has always been fine, but to acknowledge that the police service, among other partners, has to raise its game and set about the business of raising our game with all due urgency. There is nothing wrong with having a little bit of feeling behind that as well. It is implicit in the fact that we created a training video that the need for frontline practitioners, for people who might be—*[Interruption.]* Do you want me to go on?

Q6 Chair: What struck me most from the evidence that we received from David Crompton was the fact that they had no prosecutions this year for child grooming and child abuse?

Peter Davies: Yes.

Q7 Chair: Not only that, but he said there were only eight officers now in Rochdale dealing with this issue. But we have heard that since Yewtree began, they now have 30 serving Metropolitan police officers dealing with those allegations. I just wondered about that, and the Committee, I think, were concerned that the expertise was not getting out to the 43 forces.

Peter Davies: Yes. I think Mr Crompton was referring to the very specialist officers dealing with very little else except grooming and child sexual exploitation, and if he did not at the time, I am sure he would have wanted in hindsight to point out that, of course, they can be supported by a number of other officers and staff from South Yorkshire police to deal with some of these inquiries. Indeed, those who do these inquiries can get support from CEOP, from the United Kingdom Human Trafficking Centre, from SOCA and, in future, from the NCA. The other observation I would make is that prosecution is not the only measure of success here.

Q8 Chair: What is the other measure?

Peter Davies: There are a number of measures, and effort does not always result in successful prosecution. These are very complex, very time-consuming inquiries and they are a considerable investment of resources. For all their importance, they are not the only job that the Chief Constable of South Yorkshire has to do.

Chair: Sure.

Peter Davies: He has to make decisions about apportioning his resources accordingly. But my point is if that, for one year, there have not been any successful prosecutions, I do not think that is the same thing as them not having done any work in this area, because sometimes these investigations can take significantly more than a year to come to fruition. In answer to your question about what the other outcomes are, equally valid outcomes are that children who are in these hugely vulnerable situations are rescued from them, safeguarded and protected and move on to be survivors of victimisation rather than ultimate victims.

Q9 Chair: But we do not have statistics on it all, do we? Who would have the statistics? Although the previous witnesses are going to write to us with information they have, you are very clear that if we come to you and ask about the number of people involved in online grooming, you will tell us.

Peter Davies: Yes.

Q10 Chair: It is a pleasure taking evidence from CEOP because they seem to have their information at their fingertips and they tell Committees and the House what is going on. There seems to be an absence of those facts and figures, maybe not conclusions, and I accept what you say—this takes a long time—but the facts and figures that are necessary for the public to be reassured.

Peter Davies: Yes. I am very grateful for the positive comment about CEOP. I was present for the previous evidence. I think we clearly identified last year in our thematic assessment, and through ongoing work—and I am sure the Children’s Commissioner for England, when they publish their interim report in November, will identify—that there is still a way to go before really reliable national data collected to a consistent standard are available on this phenomenon.

Chair: Yes, thank you.

Peter Davies: So, I would not put myself forward as being the person who has all that data for a number of different reasons, which I think you know.
Chair: We accept that.

Q11 Mr Winnick: What evidence is there, Mr Davies, of the internet being used by groups and gangs—criminals of the despicable variety—to groom children for sexual exploitation?
Peter Davies: I think here we are getting into a difficult area where if we are not careful, we can over-categorise things and fail to see the joins. I think I am right, Mr Winnick, in understanding that your question is about the extent to which these groups, who engage in something that is loosely called localised grooming, also use the internet to do so, or is it a wider question about how many people?
Mr Winnick: The former.
Peter Davies: Thank you. The truth is that social networking and mobile data and mobile communications are pretty much universal for children and young people who, of course, fall victim to this kind of thing. We have plenty of cases where a group that targets children locally will use social networking or internet-based communications as an integral part of what they do. My professional view though is that it is an adjunct to a pattern of offending that is really based on spotting vulnerability in local areas offline. It is a tool in their toolkit, but it is not the primary driver of what they are doing. That remains, in my view, identifying children who are vulnerable almost in a physical sense—seeing what their habits are, seeing where they are and engaging with them face to face.

Q12 Mr Winnick: Given the very nature of social media, is there any firmer action that could be taken by the authorities, by the police, by Government?
Peter Davies: That is a massive debate. The Committee are moving on to the communications data legislation, which, I suppose, is approaching that question from one particular angle. There are ways in which legislation might increase the responsibility on service providers and on communicams from service providers to be more vigilant in looking for grooming activity on their networks and have an obligation to report it. To be fair, on a voluntary basis, we have a very good relationship with the majority of service providers. They support something called the Internet Watch Foundation that does a lot of very good work to take down and deny people access to images of child abuse, for example. Against the extra bits of legislation that could happen, there has to be weighed the fact that there is freedom of speech, and people do not take kindly to legislation that can be seen as censoring or restricting access to the internet.

Q13 Mr Winnick: It may be not the solution after all.
Peter Davies: I am not sure it is the solution. I think we need to tackle the human behaviour. Actually that is a truism about just about everything CEOP does. It is about human behaviour; the fact that it takes place now on the internet does not take away that our main focus is human behaviour in all its unpleasantnesses.
Mr Winnick: One would have to be an incurable optimist to believe that human behaviour is going to change to that extent. It is a question of dealing with what undoubtedly is a form of criminality. Thank you very much, Mr Davies.
Peter Davies: Thank you.

Q14 Nicola Blackwood: Mr Davies, you mentioned earlier that just having no prosecutions for one year is not an indicator of no action being taken by a police force, which clearly is the case. We do not want to discourage police forces that are taking action in this area. But clearly there has been an ongoing problem with very few prosecutions for a long period of time, not just for one year. Would you agree that there is an ongoing problem with not just police forces not recognising the problem, although some are taking action now, but also the CPS not wanting to prosecute, not finding witnesses credible and feeling that it is difficult to get evidence that would hold up in court?
Peter Davies: Yes, I would agree. It is a whole range of issues. It is not just about police forces, although that is where I can speak with most authority. It is fair to say that the investment in training and resource that was explained by Chief Constable Crompton is a good step forward and the picture I have from policing is that it is developing at a pace in terms of tackling this phenomenon. We are going to move that along with a further action plan on behalf of ACPO to make sure that the right steps are in place in every force and the right tools are available to every force. But yes, of course, one of the aspects of this is that it is hard to prosecute. We know that victims occasionally do not realise they are victims until quite late in the exploitation process. They are often selected for their vulnerability, and paedophiles generally select victims partly because they would make poor witnesses and would not even have the confidence to report. The prosecution service have to make decisions based on the realistic prospect of conviction and what is in the public interest. On both those counts, it can be difficult to balance the best interests of the victim.

Q15 Nicola Blackwood: Yes, that is true. But given that the Director of Public Prosecutions has himself accepted that there needs to be a review of the way in which the CPS handles these cases, I think that we can accept that there is significant room for improvement.
Peter Davies: Yes, and I think the room for improvement in the CPS will be the ready availability of sufficient specialist expertise to the prosecutors who have to assist and direct in these investigations and make charging decisions and prepare prosecutions.

Q16 Nicola Blackwood: Can I take you back to some of the comments you were making about online grooming? We received evidence from the Children’s Commissioner, Sue Berelowitz, who explained that her inquiry had found evidence that online pornography was exacerbating the problem of child sex abuse by normalising abusive behaviour. Can I ask whether, in your professional opinion, that has been your experience, given that CEOP not only has experience in online child abuse but has also moved more recently into child sexual exploitation?

Peter Davies: In my professional opinion, the level of exposure to pornography that is available on the internet can be harmful for children who access it, and actually can be harmful for anybody who is vulnerable to that kind of thing. Clearly, it has a role to play in normalising or making people think that some types of behaviour are appropriate when actually they are not. I do see it as an issue. My professional view is that there is work being done on that, and I do not see it as the overriding driver behind child sexual exploitation. It is a risk, it is a concern, but there are other bigger factors at play.

Q17 Nicola Blackwood: What is your view of the proposals to put in place upstream filters? There are two areas. I do not whether if you are able to answer the first question. Do you think that it would be technically possible and, secondly, do you think that it is the best answer to deal with the problem of easily accessible pornography that children can find on the internet?

Peter Davies: I have no problem with the concept; I know that some do, but I personally do not. The issue for me is it could be technically feasible to put it in place but I do not think we should underestimate the ability of people who are able and adept at operating the internet to get to what they want to get to regardless of what filters are put in place. I see it as a useful risk mitigation measure if it proves to be acceptable. I do not think it will stop pornography falling into the hands of children, for example, nor will it, of itself, stop the circulation and availability of child abuse images.

Q18 Nicola Blackwood: Is that your personal view? I know that you work with a number of partners like Google and Facebook and so on; would that be the sort of position that the partners within those organisations take or not?

Peter Davies: I am not sure they would take the same position. They might have a different view about the advisability and feasibility technically of doing it. My personal view is that anything is technically feasible if you really want to do it enough. The issue for me is that I do not think, of itself, it would stop children having access to pornography, which I think is what people would like it to do. Children will find a way on the internet just as, frankly, those that wanted to generally found a way before the internet existed. As a risk mitigation tool, I have no problem with it and I think it will help some children by denying them access to material that they should not see. I do not think it will stop children accessing pornography online.

Q19 Nicola Blackwood: What is a better way forward?

Peter Davies: I do not see anything wrong with that as part of a wider way forward. Another equally essential part of the way forward is doing the kind of thing that CEOP does, which is educating children who will be exposed to material, who may well be exposed to material, whether we like it or not—educating them to understand what is going on, to understand the risks involved in their activity, and to understand what to do if things go wrong or if they have concerns.

Going back to my previous point to Mr Winnick, we are dealing with human behaviour. I do think human behaviour can be changed and one of the best ways of doing that is giving human beings better information and better thought processes about these things. I do not see any problem with what is being proposed in terms of denying some children access to pornography. That will not be the whole answer; we will still have to end up sitting down having proper conversations with our kids about how to deal with that material responsibly because it is still a risk that they might access it.

Q20 Bridget Phillipson: Apologies for missing the first part of your evidence to the Committee. What role do you think that web hosts and ISPs should have in identifying and removing indecent images of children?

Peter Davies: At the moment, there is general support for the Internet Watch Foundation, which has a role on their behalf of circulating reference numbers of websites that carry illegal imagery, and basically denying people access to them. Within the United States, by way of comparison, there is legislation that places an obligation on service providers to report incidents of child exploitation to a receiving centre, and a slice of those reports come to the UK. It may well be that we will want to place a further obligation on service providers to report it than is currently the case in the UK. It may well be that we would also want to place some expectation on them to look for it more proactively than may currently be the case. I am no legislator, but those would be the two key areas where we could possibly look for more from the industry.

Q21 Bridget Phillipson: That certainly sounds like a sensible approach, which could lead to the outcomes that we all want to see. Do you have any understanding as to why we have not gone down that route so far?

Peter Davies: I do not really understand why we have not gone down that route so far. Having some awareness of what it took to get the US model into law—the Protect Our Children Act 2008—I do not underestimate the difficulties in doing so, and I think that came about partly by a happy set of circumstances whereby both the main parties actually ended up agreeing on that piece of legislation. I am simply speaking from a practitioner's point of view of what would help. I do not underestimate the difficulty of it.

Bridget Phillipson: Thank you.

Q22 Chair: Following on from what Bridget Phillipson said, an FOI request revealed that five police forces had seized 26 million images of children on the internet. Only 2,312 people were arrested for those offences. Your own figures show that there were 50,000 indecent images on peer-to-peer networks. That is roughly seven times larger than the 7,200 names that came over in Operation Ore. It may sound as if we are just keen to prosecute everybody we can, but at the end of the day how do you actually prosecute that very high volume of people in order to stop the indecent images of children appearing? These are phenomenally large figures.

Peter Davies: They are phenomenally large figures and, from my point of view, if it was possible to investigate every single one and prosecute every single one, then I would be perfectly happy to do so.

Q23 Chair: But is it right that you have been trialling the sending of letters to people to say, "We notice that you have been on to the website, you have accessed indecent images, please stop"? Is that what you are doing?

Peter Davies: No, it is not what I am doing.

Q24 Chair: But have you heard of that?

Peter Davies: I have heard of that. If I can just continue with the previous issue, this is criminality. It needs to be addressed as criminality. Just because lots of people do it, it does not reduce the level of criminality it represents. Actually, the report that we put out in June this year identified a pretty strong link between the possession of child abuse images and the risk of somebody being a contact abuser. It is criminality in its own right, it is a re-victimisation of the children whose abuse is depicted in the images and it is an indicator and risk to the public, and I would love there to be the capacity to do more about it. In the absence of that capacity, and I think the National Crime Agency might increase that capacity from time to time, we have to prioritise. Within that population there are people who are clearly posing an extremely high threat to children, and that is where we direct our efforts. The initiative that you are describing was an attempt by one police force, possibly two, to deal with all the other people who, because of prioritisation and resources, cannot be tackled any other way. It was a pilot scheme and it was done under very controlled circumstances.

Q25 Chair: Was it successful?

Peter Davies: I have not seen evidence of its success and I would not be recommending it to other forces to try. But let us be very clear, from my point of view, it is probably better to do something about these people than nothing. I would prefer that we had the capacity to investigate these people for the criminals they are, and arrest and prosecute them in every single case.

Q26 Chair: But as Nicola Blackwood says, you have a very good and strong relationship with the internet providers.

Peter Davies: Yes.

Q27 Chair: Why are we not asking them to do more to remove these indecent images of children from the internet? They seem to have no responsibility for any of this. They put it out there but they are not actually doing anything, are they?

Peter Davies: The service providers can obviously speak for themselves. If I paraphrase what many of them would say, it would be that they are not responsible for what goes on in their pipework, they just provide the pipework—if I can use a plumbing analogy. I do not really buy that entirely; I think they have some level of corporate and social responsibility. We have quite a good relationship operationally with many of the organisations that we might have in mind. Where there are things they can do to help, within the law and within their own legislation in the home country in which they are based, they are quite amenable to doing that. If you had some of these service providers here, they would talk you through some of the difficulties of actually taking that level of control. I think it is important to emphasise that these are not people who demonstrate no moral standing at all; every service provider is different, and the extent to which they are prepared to take steps is different and we have to deal with them on an individual basis.

Q28 Steve McCabe: Can I ask about the question of resources? You touched on it by saying you have to cut your cloth. What is the position? Do you have broadly adequate resources to deter and detect offences against children, or are you woefully ill-equipped?

Peter Davies: We ourselves, as a centre, have a pretty stable resourcing situation. We are subject to the CSR and what we have been able to do through a modernisation process is actually increase the number of people in the centre while taking on board a modest budget cut. The wider issue is that we do everything we do as a centre through a range of other partners. Any member of a police force is potentially one of our partners in protecting children. We have 70,000 or 80,000 volunteers in classrooms who take our education products and deliver them to children. Within the centre, our resourcing was never designed to be adequate to take on the whole problem. I think it is adequate to take an approach to the problem in the way we are currently doing. I look forward to the extent to which the National Crime Agency gives us new opportunities to engage more resources from the agency when necessary to mount some more operations. I think the key to the success that CEOP does have is in our understanding that the effect we deliver is generally through other people, which places the emphasis less on what our budget figure is—although it is still important to have a minimum—but actually far more on the quality of the relationships we have, the synergies we can realise and the extent to which we can persuade other people to get involved in our business as well.

Q29 Steve McCabe: So CEOP, for what it does, is adequately resourced. Were you hinting there that the cuts these other people—the other police forces and education services—are receiving are going to make it more difficult for them to do the extra part of the work?

Peter Davies: No, I was not hinting that.

Steve McCabe: I wanted to understand.

Peter Davies: I understand the question, I welcome the question. The observation I make on that is that I regularly check in with a network I have of heads of public protection units in police forces up and down the country, asking them what is happening and the extent to which austerity is affecting them. Very reassuringly, the general message I get is actually that resources are being upheld and re-thought in terms of how they are used within public protection, and it seems to me as if public protection and the protection of children is still something the police service is keen to hold up regardless of austerity. That is the general picture, so it is quite encouraging.

Q30 Steve McCabe: Okay, thanks. Can I ask one last thing? I read somewhere that the budget for the National Cyber Security Programme is about £650 million, of which approximately £65 million goes to the Home Office to deal with online offences. Is that the right balance?
Peter Davies: That is a very difficult question for me to answer.

Q31 Steve McCabe: Well, in your opinion?
Peter Davies: In my opinion, given what the money is for and knowing how it has been spent, the part that has been allocated to the Home Office is fine. Cyber-crime is like many other aspects of what I deal with; you could invest any amount of money in it, and if the overall pot is £65 million, and your question is, "Well, is it right to apportion a certain amount to the Home Office?" I have no reason to think it is not, and I have seen some of the benefits that it has delivered. But if you are in the business of child protection, there is always more to be done than the resources will allow, however much you have, and we have to prioritise, work smart, make the best of our partnerships and make the best use of the resources we do have.
Steve McCabe: Okay, thank you.

Q32 Nicola Blackwood: I wanted to follow up on your answer to the Chairman on the issue of what you do when you find a very disturbing image online of a child who is clearly being abused, and exactly how you follow that up and gather evidence to an offence because clearly you do not know where that child is or where the offender is. It is quite a simple question, but could you walk the Committee through that so we could understand your process?
Peter Davies: Nowadays, we get about 1,500 referrals a month to CEOP, some of which will be the kind of pictures that you talk about. We open them, record them, risk assess them within 48 hours and decide whether, firstly, they portray a child being at risk and, secondly, what initial investigative steps are required. I am consciously slipping into my next Committee, but let me just take the opportunity to tell you how important it is that there is proper retention of and access to communications data to enable us to do that work.
Moving on from that, it depends how difficult it is to identify the child. I have known of cases—one of which came to fruition recently—where we tried just about everything to identify a child. We finally managed to do it, found the geographic location, passed the intelligence on to the local police force who did a really good intervention that safeguarded at least two or three children and will doubtless result in some prosecution in the future.
Each image is different. Some of them have been in circulation for some time, in which case our job is to know who has already had it. But we keep these images and we examine them and look at their usage for any sign—any opportunity to identify the child depicted. Some of the lengths to which to some of the team go is quite extraordinary. It is probably not for the public domain, but if the Committee has an opportunity to visit, then you will see some of that for yourselves.

Q33 Nicola Blackwood: Do you think that there is a need for legislative changes, other than on the communications data that you already mentioned, in order to enable you to effectively prosecute in this area? Are there any gaps?
Peter Davies: If there was one piece of legislation that would help us, it would be the retention of and access to communications data on an organised basis. Anything else is at a long distant second level of importance. There are some ways in which the legislation that, for example, enables preventive orders to be put in place for sex offenders could be changed, because the current array of opportunities is not hugely well used and does not always follow the people who pose the biggest risk. I think the legislation is pretty adequate for the job; there are not any glaring gaps. It might be worth looking at whether we should seek to criminalise what you could call the written word that is clearly paedophilic and predatory in nature, in the same way as we criminalise child abuse imagery and virtual images of children. That is one area in the online world where the legislation could be improved but, mark my words, it would be nothing like as important as making sure that we get communications data back to identify victims and offenders, which is currently, to some extent, a lottery. That is the big game at the moment, and it is really important to understand the relevance of that to child protection.
Nicola Blackwood: Okay, thank you.
Chair: I am sure you will continue that at the next Committee.
Peter Davies: Indeed.
Chair: For which you are very late at the moment.
Peter Davies: Good heavens. So I am.

Q34 Chair: Mr Davies, thank you for coming in. One final thought, as this inquiry goes on, we are concerned by the lack of co-ordination and it may well be that CEOP ends up in the NCA as doing more than just online protection.
Peter Davies: Yes.

Q35 Chair: We have heard some very good witnesses throughout this inquiry but it still lacks that one central point. In a very brief answer, do you think that is right—that we need to move in this way? We have 43 forces doing different things, with different expertise, the Human Trafficking Centre, SOCA doing its bit or the NCA doing its bit. There you have a degree of expertise that is unrivalled in your organisation. Maybe this is the way forward.
Peter Davies: Yes. We already go beyond the online, and actually group-related child sexual exploitation is

one of the five priorities for the centre this year. Whether the national leadership comes through ACPO, or through a CEOP command with the National Crime Agency, greater coherence and clearer leadership are things that would be usefully brought to bear on the situation. From my point of view, the NCA and the national coordination tasking model provides a useful model through which that might be done.

Chair: Sure. Mr Davies, thank you very much for coming today.

Peter Davies: My pleasure, thank you very much.

Tuesday 20 November 2012

Members present:

Mr David Winnick (Chair)

Nicola Blackwood
Mr James Clappison
Michael Ellis
Dr Julian Huppert
Steve McCabe
Bridget Phillipson
Mark Reckless

In the absence of the Chair, Mr Winnick was called to the Chair.

Examination of Witnesses

Witnesses: **Deputy Assistant Commissioner Martin Hewitt**, ACPO e-crime lead, and **Deputy Chief Constable Peter Goodman**, regional e-crime lead for East Midlands, gave evidence.

Q368 Chair: Mr Goodman and Mr Hewitt, good afternoon—I do not think it is quite good evening as yet. The Chair has had to leave for various reasons, but we are grateful to you for coming along.

The globalised nature of e-crime is often cited as a major barrier to identifying those responsible and bringing them to justice. How are the United Kingdom police building a relationship with their counterparts in dealing with what is undoubtedly an international menace? Would you agree it is an international menace?

DAC Hewitt: Most definitely. It is fair to say that trying to ascribe a region around cyber crime is challenging in itself. You will hear talk about force level or national level or regional level, and actually the vast majority is international in its nature in terms of where the victims are, where the perpetrators are and where the systems they are using are. Inevitably we have to find a way of dealing with this in investigative terms and preventative terms that works across boundaries.

The Government has ratified the Budapest Convention, and we are supporting the EU Cybercrime Centre that is being set up in Europol, but primarily from our perspective the Police Central e-Crime Unit, which is the main operational unit that is hosted currently within the Metropolitan Police, has developed very strong relationships with most of the key countries and law enforcement in the key countries with which we work, and the Crown Prosecution Service does likewise with the prosecuting authorities. There are undoubtedly significant issues because you get into cross-jurisdictional issues that can be quite challenging for us. There are, with certain countries, logical levels of trust issues in terms of how much we are able to share and how much they will share with us, and it is just the number of players that can be involved in operations.

We are working well with others, but there is no doubt that this is an area where I think globally we need to move forward in terms of how we allow ourselves to work across jurisdictions and to gather evidence quickly, which is one of the biggest issues for us because generally we would work through the normal mutual legal assistance process. That can be very slow in what are often quite fast-moving investigations. It is about those police-to-police relationships, but I think globally we need to move forward in terms of how we deal with this challenge.

Q369 Chair: There was an error on my part. I should have asked you to identify your name, rank and responsibility.

DAC Hewitt: Sorry.

Chair: No, that is my mistake.

DAC Hewitt: I am Martin Hewitt, Deputy Assistant Commissioner within the Metropolitan Police Service. I work within Specialist Crime and Operations and have the chief officer oversight for the Police Central e-Crime Unit. I am leading for ACPO on the migration of the e-Crime Unit into the National Crime Agency.

DCC Goodman: I am Peter Goodman. I am Deputy Chief Constable for the East Midlands. I serve the five forces of the East Midlands around counter-terrorism, serious and organised crime and major crime. In relation to cyber-criminality, I have led on the project to deliver the regional hubs in three locations across the country, and I am just about to take over the national cybercrime portfolio that was vacated by Janet Williams on her retirement.

Q370 Chair: Thank you. Before I ask any further questions, is there anything you want to add, Mr Goodman, to what Mr Hewitt has said?

DCC Goodman: No, there is not. We have discussed beforehand.

Q371 Chair: I see. I will not describe that as a conspiracy in any way, shape or form. One assumes that the counterparts to the police in our country are in the main—I would be surprised otherwise—quite willing to co-operate in enforcing the law and bringing the culprits to justice, but are there difficulties now and again so far with police overseas?

DAC Hewitt: Generally speaking, law enforcement will be keen to assist but, as I say, you get into those kinds of jurisdictional challenges. One of the challenges—and we were just discussing it outside—is that certainly in most European countries, the method of investigation is run by an examining magistrate and somebody judicial, and they find it quite strange operating with us on a police-to-police basis. But it is trying to find a way we can operate within the bounds of our legislation and our procedures, and equally, so in a sense the challenges are no different than they are in any other international investigation. I think in the cybercrime arena it is pretty much there in every example, whereas in others it will be in a few. There is a challenge around how we equalise processes and allow us particularly to move evidence quickly from one jurisdiction to another to move an investigation on.

Q372 Chair: E-crime has come up for obvious reasons with all the technology involved in bringing this to the forefront. Would you say that it is going to increase substantially compared with other forms of criminal activity?

DAC Hewitt: I would say that it is, largely because what it is generally doing is either presenting opportunities for new forms of criminality that can be very profitable—and for all sorts of other motivations—or facilitating technology more generally, and the cyber-environment is facilitating existing criminality. I think one of the factors that Government agencies and everyone involved needs to take in is the speed with which it changes. We have worked in organised crime and serious crime for many years, and most other forms of serious crime will mutate and develop their methodology in relatively slow time to changes in the environment—to changes in what we do. In the cyber-world, you are talking about that happening almost constantly, and so the people who are out there are trying to find new ways and trying to overcome the defences that are being put in place within business and privately. You can only see that cyber, in its broadest definition, is going to increase because so much more of our lives are run in that space.

Q373 Chair: Which inevitably leads to the question that presumably there will be far more officers trained to deal with this.

DAC Hewitt: Yes.

Q374 Chair: Mr Goodman, is that your view?

DCC Goodman: Yes, very much so, and some of the work we have done around the regional hubs demonstrates the extra value that we can gain as a consequence of greater understanding, greater technical skills and also greater investigative techniques. This is the one area of policing at the moment where you are likely to have an offence committed in one part of the world through technology that is held in another, with a victim in a third part of the world, and that is an extremely complex environment, especially, as Martin says, because it mutates so very quickly from one form to another.

We are seeing some of the serious and organised crime partnerships of the past—criminal partnerships—that are now understanding the profit that can be got from this, so it is a very complex environment. We in the police service, together with our partners, need to make sure that we are understanding how that changes, understanding the problem and making sure we understand how we will respond effectively.

Q375 Mr Clappison: Without naming them, are there any particular countries that you find commonly tend to be involved in this sort of crime—as the headquarters for the people who are the brains behind the crime? Are you completely satisfied, if there are, with the response you get from Governments there?

DAC Hewitt: There are areas you would tend to see more criminality emanating from, and there are other areas where the technology and operating systems would tend to be. Some of those are challenging. The other important aspect to remember about cyber, which again makes it quite different to some other forms of criminality, is the range of activity that cybercrime can include. We have tended to be talking here around the kind of cybercrime for a financial profit in the fraud sense but, at the other end, you have cybercrime as hacktivism, as it will be called, and running up to state-sponsored and terrorism as delivered by cyber. All that is going on simultaneously. Another one of the challenges is some of the key actors in that activity, because of their technical skill and their knowledge, could be present in any of those different arenas, which again is quite different in its makeup to what we would normally be dealing with in either the terrorist or the crime world. But there are countries, and they will be fairly obvious, where there are real challenges with working with them. As I say, some of our challenge, of course, is in some environments it is going to be difficult for us to share information, but we have overcome that in some instances and we work very closely with a number of countries. It really is about trying to generate globally intolerance to this type of criminality and the willingness for people to share information and to take part.

Q376 Mark Reckless: Mr Goodman, I understand you are the ACPO lead on e-crime, and as I understand it, Mr Hewitt, you are the ACPO lead for the Police Central e-Crime Unit. Could you explain your division of responsibilities, the role of the Police Central e-Crime Unit, and particularly the role of ACPO in overseeing this area?

Chair: In some respects you have done that, but if you would give a fuller picture arising from the question.

DAC Hewitt: When this first emerged as an issue there was a single ACPO lead, Janet Williams, who I think has probably given evidence before you in the past. Janet was part of the original process that led to the creation of the Police Central e-Crime Unit. PCeU, as we call it, is the funded team that has grown now to being over 100 members of staff, that has the primary investigative capability for tackling high-level cyber-criminality.

Q377 Mark Reckless: Who does that report to?

DAC Hewitt: That reports ultimately to me within the Metropolitan Police, because it is hosted in the Metropolitan Police. We are in a process of transition at the moment and, ultimately, PCeU will become part of the National Cyber Crime Unit that will sit within the NCA when that is created in about a year's time. We are in a transition process at the moment and what will then happen is a cyber-capability will remain, obviously, in the Metropolitan Police for dealing with specific issues there, but the responsibility for being the top-level investigative capability will transition across to being within the National Cyber Crime Unit within the NCA.

I have the operational oversight and also, having been involved in it for the past two or three years, the lead for that transition work to make sure that in capability terms we don't lose anything at the point when PCeU transitions into being part of the National Crime Agency from a national perspective.

DCC Goodman: I have picked up the strategic role from Janet Williams around the development of cyber-capability and cyber-responses around the country within the last three or four days, so I hope you will be reasonably gentle with me on the basis of that. That includes the development of the hubs around the country, their performance and the outcomes that they achieve. It is about developing a comprehensive training programme on behalf of the police service—from executive level right down to first responders—so that we increase knowledge among the police establishment. It is about developing the ways and means to enable communities, businesses and large enterprise to prevent the commission of offences against them, which have not been developed in a comprehensive way before. It is around making sure that we get our victim engagement right, because there will be many thousands of victims here who are looking for a response from us when we have yet to understand fully what that looks like.

Q378 Mark Reckless: You speak of victim engagement. We have had some engagement from the British Retail Consortium, which says that a number of its members have put an awful lot of work into preparing cases where they, and potentially other companies, have been the victims of e-crimes, but they have then been disappointed that these have not then been taken forward by the police. Can you offer them any hope for the future in that area?

DAC Hewitt: I can, I think, but I absolutely recognise their frustrations at the moment. The challenge that we are facing is, having got ourselves beginning in cybercrime and creating the Police Central e-Crime Unit, we have moved on enormously in terms of our capability and capacity to deal with things at a higher level. What we are trying to catch up with now is to get all the police forces aware of the phenomenon and capable of dealing with the phenomenon, because clearly once the Police Central e-Crime Unit transitions into the National Cyber Unit, there will have to be a threshold around the level of investigation that they undertake. The work that Peter referred to in terms of mainstream understanding, knowledge and capability around the country and in terms of training people up to have a capability and having the hubs is all designed to allow us to be able to investigate crimes at a lower level more generally.

The goal in cyber has to be around prevention activity and developing prevention activity. I know it is often rolled out, but it is the simplest image to use: we have to get to a point where we, as citizens, organisations and businesses, are not, effectively, leaving the windows and the doors open when we leave the office or when we leave the house. We have to start working much more collaboratively with business, industry and other Government agencies to make sure that everybody out there has the best information about protecting themselves in the first instance. Then we need to increase our capability to be able to investigate when a crime does occur. I know it is in some of the written evidence that you have already received, but the latest GCHQ assessment was that 80% of the criminality that was reported could be prevented with relatively straightforward security measures being taken, either by the individual or by the organisation. I think collaboratively we have to work much more closely together. We undoubtedly have to develop our ability to investigate lower level crimes.

Of course, there is another important difference, which is if someone's house is burgled, there may well be other burglaries that have taken place, but that is essentially an individual crime that the police will go along and investigate. If someone has a relatively low-level cyber attack that steals some money out of their bank account, steals their identity or whatever, the chances are that they are going to be one of many, many victims, because that is the nature of the criminality. We need to be working at understanding that picture and then getting up that chain to start being able to do the disruption and the prevention higher up.

Chair: We have a bit of a problem—for my colleagues, and also for Mr Goodman and Mr Hewitt—that I think we are going to be deserted in this Committee if we go on beyond 5 pm. So I am keeping an eye on the clock and keeping an eye on the questions and the answers. They are very informative, but we have to make some progress.

Q379 Mark Reckless: Just very quickly, the Home Office tells us that it is planning to have changes in how e-crime is recorded. Do you know when that is going to come in? Is that going to help you in your work? It may be an extra bureaucracy for officers locally to have to do that.

DAC Hewitt: The view is around changing some of the recording. As it says in the evidence there from the Home Office, there is no such thing as a cybercrime on the current recording system. We need to be very careful that we are answering the right question, because for me this is not about how many are we recording. A harassment, a theft or a fraud is still a harassment, a theft or a fraud, whether that is delivered through a cyber platform or not. The more important point for me is for us to be able to have information that allows us to understand the nature of those attacks and where they are coming from, and then allows us to work out what we can do to deal with them at that high level to prevent them happening.

Q380 Dr Huppert: Presumably in order to allocate your resources effectively, you have to know how these crimes are being committed. Do you have enough information? Would you want to see the modus operandi of a crime always recorded with the offence so that you know exactly what is e-crime that

you can tackle and what is not, and how you should allocate those resources?
DAC Hewitt: The more information we have the better. Recording the method relies on a level of knowledge within the victim and a level of knowledge within the person who is receiving the report to do that effectively, but I think we are trying to get towards that. The key issue for me is using as many reporting mechanisms as possible, so some of this will come through crime reporting and some of it needs to come through our relationship with business and industry who are informing us of attacks that they have fallen prey to or that they have successfully prevented, and then it is building as much information as we possibly can about the methodology, who the victims are and the nature of the information, because it is normally data that people are trying to get to in the first instance. All that allows us then to work again with partners, both public and private sector, to identify the way that you can either block that methodology or tackle or investigate. The more information the better, but I don't think necessarily the answer is going to be just having more expansive MO submissions on the crime reports.
DCC Goodman: Just to add on the back of that, it is interesting that we talk about crime recording and, of course, we ought to move to a process where, wherever possible, we understand the part that cyber has played in a particular type of criminality. One of the big stumbling blocks to that is that often the victims of that cyber-criminality won't know—and they certainly won't know—the detail of what has been committed against them. A victim of a dwelling-house burglary will tell you they came in through the front transom window and they stole the video recorder from the lounge and they went out via the front door. It is very difficult for a victim, even if they discover it, to understand how £200 has gone missing from their personal account, so it is not without complexity.

Q381 Dr Huppert: Let me come back to the issue of resources but just pick up on this issue about the victims. As I understand it, you currently have the Police Central e-Crime Unit, SOCA and CEOP, and you have the City of London Police, which has a role on internet-enabled fraud. If I am victim, who do I go to? Do you seamlessly pass people from one group to another, or are there silos, as happens in most other areas?
DAC Hewitt: In the first instance you would go to your local police force. The process, as you will be aware I am sure, with Action Fraud, which sits within the National Fraud Intelligence Bureau, is developing a process to take some of the cyber reports as well to try to build the picture.

Q382 Dr Huppert: Do you think that is working, by the way?
DAC Hewitt: I think it is a start, and we need to get to a point where we can get a bigger picture of what is going on. I think the system at Action Fraud is not designed to give the real granularity of detail about individual offences, but what it can be, hopefully, in the future is part of the broader picture of the offending type. Do we pass a victim seamlessly? Sadly, probably the answer to that would be no, but that is the work that Peter is doing around information for officers. Now cyber-awareness will form part of pretty much every basic and advanced investigative course that police officers do. There is a whole range of electronically delivered awareness training. It is all about building that picture up and then being able to, I think most importantly, give a victim a very honest picture of what that experience is going to be and what they are going to get as a result of reporting that crime, but it is not seamless at the moment.

Q383 Dr Huppert: I think we will be making some suggestions about that. Can I come back to the money issue? In the whole National Cyber Security Programme, I think 10% of the money—£63 million—is given to the Home Office to tackle e-crime. Do you think that is the right balance in terms of the whole National Cyber Security Programme, and what are your priorities for spending that £63 million?
Chair: I think that Mr Goodman is suggesting that is a lead question for you, Mr Hewitt.
DAC Hewitt: Coming from pretty much a standing start, that was probably the right sort of allocation of money to allow us to develop and understand the capability we needed to develop, and then the capacity. A large part of that money has gone to creating the Police Central e-Crime Unit and developing that capability and capacity. We have the three regional hubs now up and running. It is about all the development of the training to mainstream cyber-understanding as part of law enforcement training for anybody who works within law enforcement. We have high-level accredited training. We have started to try to understand how we manage digital forensic processes as well. One of the challenges you have at the moment—unlike when I was originally going in and searching people's houses when I arrested them—is when you walk into someone's house, there will be probably five or six electronic devices that are essentially computers. It is how we understand and how we better triage what we submit for forensic examination, because otherwise the system gets clogged with what questions we are asking the providers to give us. It is work around forensic, work around crime reporting and work to try to develop the virtual taskforce working with business and industry, but the significant point for me is we cannot solve this issue as law enforcement. This will only be solved by Government, law enforcement and other agencies all bringing to bear their abilities and then working with business and industry.
Chair: I think that is a very valid point indeed, and I am glad you have mentioned and emphasised that.

Q384 Dr Huppert: One last very quick question. We have talked a lot about resources and setting up the infrastructure. Are there any legal powers that you need, or any legislative changes that would make a difference, or is it largely about resources and training?
DAC Hewitt: There is work under way to review the Computer Misuse Act, which I would say is not fit for purpose now. It is a fairly old piece of legislation, and,

as we said, this is changing very quickly, so that work is under way as a review.

Q385 Dr Huppert: That is the main one.
DAC Hewitt: Yes, from my perspective.

Q386 Steve McCabe: Mr Hewitt, I understand that the Cyber Security Strategy requires you to mainstream cyber-awareness and skills through the police service. How do you measure your success in doing that?
DAC Hewitt: In the first instance, the reality is you measure it by the output and the delivery, and, as I said, we have a programme now that takes you right from being newly appointed and from being a trained police officer through all the investigative stages that a person would go through in their career, with cyber being part of that, right up to the training for very senior officers. In the first instance, it is going to be about measuring the fact that we have created those programmes and that they are being delivered and everyone is undertaking them. As we move forward, the measure will be whether we are more effectively dealing with the issue and, as was previously asked, whether, when someone walks in and report a cybercrime, we are dealing better with that than we currently do.

Q387 Steve McCabe: Mr Goodman, you have mentioned the regional e-crime hubs. Just succinctly, what are the goals of e-crime hubs?
DCC Goodman: They set out to achieve three main goals. One was to increase the strategic capability we have across the country because there was no real accredited capability developed outside London before they were delivered. We now have that in three locations—in the East Midlands, in the North West and in the Yorkshire and Humber region—but they don't just service those regions. They service the entirety of the country in a very strong partnership with the Police e-Crime Unit. Secondly, it was to start to develop some of that tactical awareness among officers around victim care and around the methodology that they can adopt. Thirdly, it is very much around raising awareness, not just within the law enforcement community but among broader communities of the prospect of cyber-criminality and the means of preventing some of that taking place.
Steve McCabe: That is lovely. Thank you very much.

Q388 Mr Clappison: On the definition of e-crime, do you think that crimes that use the internet only for organisation or communication—other types of crime that is—be categorised as a type of e-crime, or do you think that just conflates the issue?
DAC Hewitt: My take on this is we are in danger of asking the wrong question. The reality is, as I think I said in one of the earlier answers, that there is going to come a point where almost every crime that takes place has some involvement of some form, and I wonder what we achieve by doing it. I would rather get us to a point where we understand the impact of technology on crime, whether it is what I would call a pure cyber right down to, "I used my device to facilitate it", and then we understand what it is we need to do to deal with that—either to prevent it or to detect it. The danger is that we go down a route of wanting to define things when, quite frankly, the criminals out there are not thinking about that. They are just using whatever method is the most convenient to do the crime.
Mr Clappison: That is very helpful. Thank you.
Chair: Gentlemen, undoubtedly there will be further sessions, and we will be calling other witnesses. It may well be the Committee, or the Chair in particular—who, as I have said, is not able to be here—will want to write to you and ask further questions, but we are most grateful to you for coming today. It is a new field for us—perhaps more of a new field for us than it is for you—but it is one which certainly this Home Affairs Committee is going to explore, hence the reason we were very pleased you were able to give evidence today. Thank you very much indeed.

Tuesday 11 December 2012

Members present:

Keith Vaz (Chair)

Nicola Blackwood	Bridget Phillipson
Michael Ellis	Mark Reckless
Dr Julian Huppert	Karl Turner
Steve McCabe	Mr David Winnick

Examination of Witness

Witness: **Commissioner Adrian Leppard**, City of London Police, gave evidence.

Q57 Chair: Mr Leppard, thank you very much for coming in. Apologies for keeping you waiting.
Commissioner Leppard: Thank you, Chairman.
Chair: As you know, the Committee is conducting an inquiry into e-crime, and we are hearing from a number of stakeholders. You obviously have the lead in respect of this area. How big is the team that you have working with you, and where are you based at the moment?
Commissioner Leppard: City of London Police has about 13,000[1] people altogether. About 250 people specialise in fraud and economic crime, and the roles we have are dedicated fraud investigation teams, but for this meeting in particular, we also host the National Fraud Intelligence Database, the one single repository of all reported crime intelligence from the police, members of the public and the private sector.

Q58 Chair: Will you be keeping that under the *New Landscape of Policing*?
Commissioner Leppard: Yes.
Chair: Why?
Commissioner Leppard: Because we have effectively built very good relationships with the private sector, and personal data-sharing relationships. We have highly skilled officers. We have a good track record of taking cases to court, and in the discussions we have had with the National Crime Agency, there is nobody who can see any benefit that we would gain by moving any of that to another agency. It would not increase efficiency or effectiveness, and it would cost more.

Q59 Chair: It is interesting because, of course, the Committee is concerned about *New Landscape of Policing*, which has not been completed; it is an unfinished masterpiece of the Home Secretary's. We were concerned about the very same arguments you have just mentioned. As far as CEOP was concerned, the previous director of CEOP made the same arguments that you have made—that, "It is better outside because we have relationships with the private sector and we want to continue with it", but CEOP was included in the National Crime Agency. Everything else to do with e-crime is going to be in the NCA. That is right, is it not? Would it not have been sensible to put them all together? Either give that function to you and the City of London Police or take your functions and put them in as part of the NCA?
Commissioner Leppard: It is absolutely sensible to have the debate, and I think what we focused on is, where is the added value? Where is the added benefit?

Q60 Chair: Sure. But the debate is over because the decision has been made already.
Commissioner Leppard: It has. If I may, Chair, as you know, under the National Crime Agency there are four commands. Three of them—CEOP, Organised Crime and Border Police Force—all have their own assets and agencies. There is a body there. Economic crime does not, and we will represent policing. Of course there are many other agencies, like the Serious Fraud Office, the Office of Fair Trading and many other agencies that all have to work together, and the challenge of that particular command will be to get the best benefit.

Q61 Chair: Is there an argument to give it all to you, since you are doing such a good job? We will examine your job in a second, but since you appear to be doing such a good job, is it not better to have one function, the e-crime function, in the City of London, where you have your specialists, rather than have them put into the NCA, which is at the moment, as I have said, incomplete?
Commissioner Leppard: Chair, I do not agree with that, no. I think the way it functions at the moment, with us representing policing, one part of the agency under the economic crime command, and hosting the intelligence function, and then working very closely to the strategic priorities of the National Crime Agency, is probably the most effective way to work.

Q62 Chair: Let us turn to some of the results. The British retailers have said that online internet crime reached £205 million last year, and the global economy loses about £114 billion due to online crime. Are we winning? You have heard the argument, "Are we winning the war on drugs?" There are different arguments on that. But, as far as e-crime is concerned, are we winning this battle? Almost every week we have another example of somebody breaking in. The Home Office website was the last time somebody broke into something official. Who are these people who keep, in effect, running rings around some of the best police officers in the country?
Commissioner Leppard: The direct answer to your question is we are not winning. I do not think we are

[1] Note by witness: The Commissioner actually said £1,300 during the session, however after checking figures £1,100 would be a more accurate figure.

winning globally, and I think this nature of crime is rising exponentially, which is clearly why you are here and asking these questions today. As a country, we are as far advanced as any other European country, and indeed anywhere else in the world, but we are new in our development. I am sure you have heard evidence already from the cyber crime strategy, the new money and development. This Government has put a focus on economic crime. We have a focus on cyber. Many other countries have not, but we do have to bring all that together, and that will take a couple of years.

I have many facts and figures, which I can give you, about the nature of the scale of the threat, in terms of cyber and organised crime.

Q63 Chair: Yes, we are coming on to some of that. In terms of identifying countries, is there a particular country or group of countries where, when you arrive in the morning at City of London Police, you say, “My goodness, there is something else coming from this country. They obviously have the expertise to try to challenge what we are doing”?

Commissioner Leppard: There are countries in terms of the nature of the threat we are facing.

Q64 Chair: Could you give us an example?

Commissioner Leppard: To give you the nature of the threat that we know in the National Fraud Intelligence Bureau, we map organised crime groups and we know that about 1,300 of those groups are doing nothing but fraud as their main means of gaining money, as a criminal enterprise. A good 25% of them are using cyber as their main means—in other words, internet-enabled criminality. The work we have done to identify countries shows that about 25 countries predominantly target the UK.

Q65 Chair: Give me the top five.

Commissioner Leppard: The top five are mainly eastern European, and Russia is another country that we know hosts some of the criminality. That is not the Russian Government, but the criminality is hosted in that country.

Q66 Chair: In terms of the eastern European countries?

Commissioner Leppard: We have countries, such as Romania and others, which we are working with. With all these countries we are working with the law enforcement agencies, but I am trying to give Members of the Committee a picture of the nature of the criminality.

Q67 Chair: Sure, absolutely. You are obviously creating partnerships with the law enforcement agencies in those countries, to try to challenge the criminal elements from Russia and eastern Europe who seek to attack us through cyberspace.

Commissioner Leppard: Yes. Two challenges are really important for us. One is about how we deal with prevention. The other is in terms of cyber crime. By “cyber crime” I mean not just the technical attack but the fact that internet enabling is allowing a lot of fraud to be perpetrated across borders. A big challenge for us as a country is understanding the international threat and what the UK Government can do, with law enforcement, to try to gauge more effectively in other countries to combat that threat.

Q68 Chair: I was in Washington in the summer, and in the meetings that I had one was specifically about cyber crime and e-crime. The Americans certainly seemed to be very worried, and President Obama seems to be extremely worried, about this type of crime. Are the Americans working with us on things? Are they more advanced than we are? Do they have more resources? Are they more likely to be under attack than we are?

Commissioner Leppard: I think all of those things, Chairman. They have more resources. They are likely to get more attacked because of the nature of the scale of the business they have. In terms of the specialisms, we share a lot of knowledge.

You will hear from Charlie McMurdie from the Police e-Crime Unit that we have as much knowledge through SOCA and the Police e-Crime Unit as any other country has. But they are right to be worried about the scale of the threat, and you have heard from the British Retail Consortium. I think they have shown something like a 30% increase in online fraud attacks in the last year alone. This is a very worrying criminal trend.

Q69 Steve McCabe: Mr Leppard, one of the Government’s cyber security goals is to mainstream the capacity of police forces and law enforcement agencies to deal with e-crime or cyber security issues. How well are we doing in pursuit of that goal?

Commissioner Leppard: As you will hear from Charlie McMurdie, the Police e-Crime Unit, which has been leading on that, has been doing a good job to take training into police forces, right down to the beat officer level, to increase a better level of awareness, and there is certainly a marked difference. We have our own training capacity. We have an academy, and we train investigators in how to use the internet. If you said where we were two years ago to where we are, there is a marked difference in skills—not just of specialist fraud investigators, but all different types of roles within policing. Of course, there is still a journey to go, but we are certainly on that journey.

Q70 Steve McCabe: Are there any areas that cause you particular concern or that you would want to draw the Committee’s attention to?

Commissioner Leppard: My area of special expertise is around economic crime and fraud but, as I have said, 50% of that is now being enabled through the internet. My concern, when I look across the country, in terms of fraud expertise, is that we know that the number of dedicated fraud investigators in policing is reducing. We anticipate it will reduce by 25% over the CSR period. There are only about 600 dedicated fraud investigators in British policing and we have

200[2] of those, so the real worry is that, at a time when fraud and e-crime is going up, the capability of the country is going down.

I have had discussions with the Home Office about creating a new national capability for economic crime that would support specialist agencies, like the PCeU, that will be dedicated fraud investigators. The Home Office have been very supportive of that, and I am looking at that funding proposal now.

Steve McCabe: Thank you very much.

Q71 Karl Turner: Clearly, victims of online fraud suffer real harm—psychological harm, among other things. What is your view of sentences? Are they currently too lenient or about right? What is your opinion?

Commissioner Leppard: It would probably be inappropriate for me to comment on sentencing. Each case is utterly different, and the judicial guidelines are that each case will be considered on its own merits and the level of harm, and I know judges do give consideration to that harm.

If I may endorse your point, one of the biggest frauds that we experience on the internet is called mass marketing—that is, the selling of online shares. Some 50% of the victims of that—and it is a £3.5 billion loss—are over 65. The average loss of those people is £25,000. That is a significant loss to the most vulnerable people in our society. The only comment I would make is that I would hope, like you, that due consideration is given in sentencing to the harm that victims are experiencing.

Q72 Karl Turner: What is your opinion, though, Commissioner? You have experience in seeing cases dealt with in criminal courts. Do you believe that the judgment of the court, the sentence passed down by the judge, reflects the psychological harm done to its victims or not? Please say yes or no. Do you think it does or it doesn't?

Commissioner Leppard: In some cases it does, but in some cases it doesn't.

Q73 Dr Huppert: Commissioner, can I follow on from some of the direction of that question, and ask about how you deal with the victims of online fraud? Certainly, when I have had constituents concerned about this, the sense is that the bank requires them to prove that they were the victims of fraud, rather than regulations protecting them. What is your assessment of that balance? Is the protection the right way round?

Commissioner Leppard: There are two questions there. If I come back to the regulations, which I think are good and sound in this country, if we can get a victim through into Action Fraud, which will be the central reporting for all fraud and cyber crime in this country—as I am sure Members know, Action Fraud is the core central web centre, basically, that comes into the NFIB, the City of London Police—we then have a very extensive engagement with them, supported by the Victim Support Scheme.

We monitor their satisfaction about how they have been treated as a victim, and the percentage levels of satisfaction range between 90% and 95% of victims. That is them saying, "We were satisfied with how we were dealt with". The issue is whether we can get enough knowledge that people need to report in the first instance, and that is a constant battle to get public awareness into that. I am very comfortable that, once they are in the system, we do the best possible job to represent their interests, look after them and keep them informed.

In terms of the bank's role—you asked me specifically about regulation—I do think we have a very good regulation system in this country. There is always a challenge about whether the banks themselves and different banks are complying with all the regulations, and that is always the issue in terms of enforcement—that is probably a question better given to the Financial Services Authority, in terms of how they comply—but I think we have a good and effective regulatory system.

Q74 Dr Huppert: What steps do you take to make people aware that they ought to be reporting? Particularly for people who are not that digitally literate, who will still, nonetheless, use online banking and things like that.

Commissioner Leppard: I did say at the beginning, as well, that there are two issues. One is about prevention and the international dimension, but there is a big challenge for us. Knowing the nature of the threat at the moment, knowing it is reaching into every aspect of society, we must put a lot of energy into our public campaigning, and that is not just prevention.

There is some great work going on under the Cyber Security Strategy, very effective work in prevention. The National Fraud Authority has put on a great campaign on Facebook—you may have seen it—"The Devil's in your Details". If you have not seen it, I suggest you do. It is a great way of helping people realise what we need to do. But, as you say, if I speak to an average member of the public and say, "Have you heard of Action Fraud?" they will say no, often, until they then want to know, "How do I report my fraud?" If they have not gone on the internet, how do they find that? It is a challenge we have, and I accept that challenge. We do have to push that out in better campaigning and much more public messaging about it.

Q75 Mark Reckless: Commissioner, what role do you see for public awareness campaigns in tackling fraud?

Commissioner Leppard: We have to put a huge amount of energy into this for the future. We need to stop thinking about fraud and cyber crime as something that perhaps only affects a smaller part of our population. It is affecting everybody. The second highest reporting coming into Action Fraud is online shopping, and it is in every community now.

Yes, we have to do prevention with the private sector. The biggest payback for us as a country is working with the private sector. I would like to see more

[2] Note by witness: A review of national police fraud squad resources undertaken in Summer 2011, established that approx 650 staff investigated fraud, of which approx 190 were from the City of London Police. These are in addition to the 200 City Police resources as stated initially.

campaigns similar to those on television that you might have seen, with drink-driving or road safety, and more investment from the Home Office and other agencies with cyber security—perhaps through the Cabinet Office money—to focus into segments of society.

It is a fairly long answer but, if I may, the National Fraud Authority does some excellent work at segmenting victims of frauds and cyber, and the campaigns are targeting different groups in our society. We need to put more energy into that, I think.

Q76 Mark Reckless: When you say "working with the private sector", do you see that as distinct from a general public awareness campaign?

Commissioner Leppard: The private sector has as much interest as us in trying to reduce cyber crime and fraud commercially. You will be aware that we have done a lot of work with different sectors—the insurance sector and the banking sector—to start finding ways in which they can fund some policing activities. There must be ways we can be innovative with the public sector so that they can help, perhaps, in some of the public messaging that we are going to do, particularly in relation to funding some of that.

Q77 Mark Reckless: If you had to choose between more money for your team of officers enforcing on these issues versus money for public awareness campaigns, which would it be?

Commissioner Leppard: You would have to take a balance on that. The primary mission that I stand for is to protect the citizens of this country and, if I believed public messaging would protect more defrauded victims, then that is where the money should go.

Mark Reckless: Thank you.

Q78 Chair: There was an attack on the Home Secretary's constituency website and the Home Office website earlier this year by an anonymous cyber criminal. What sanctions will he or she face, once he or she goes through the system? Will it be jail? Will there be a fine?

Commissioner Leppard: Firstly, you need to know what offence they have committed.

Q79 Chair: But he has obviously committed some offence, if he has been arrested and charged, has he not?

Commissioner Leppard: There will be either the Computer Misuse Act or the Fraud Act; they are the two main Acts. When that person goes to court, they will be charged, clearly, and there will be a hearing, either summary or it will be at the Crown Court, and the sentencing would be dependent on the sentencing guidelines of the country.

Q80 Chair: What are they, roughly?

Commissioner Leppard: Each case, as you are probably aware—

Q81 Chair: What is the maximum for something of this kind, depending on what they are charged with?

Commissioner Leppard: It depends on whether it is an indictable offence or not, but you can get up to eight to 10 years for a fraudulent offence. You can get the same for computer misuse. It is unlikely to be anything more than that.

Q82 Chair: Al-Qaeda has advocated a cyber jihad. Have you heard about this?

Commissioner Leppard: The threat from cyber and terrorism is something we have been working on with Government, GCHQ and other agencies, for many, many years, certainly.

Q83 Chair: Do they engage in e-fraud activities, as far as you are aware, or do they just try to disrupt existing websites?

Commissioner Leppard: No, there is plenty of evidence to show that some of the financing for terrorist activities worldwide will use fraud as a means of gathering money.

Q84 Chair: Does that apply to al-Qaeda as well?

Commissioner Leppard: It does, yes.

Q85 Chair: How would you seek to disrupt that?

Commissioner Leppard: We do seek to disrupt that now. In terms of other agency responses—MI6, MI5, GCHQ—all have some of the new cyber money, and all are taking actions to disrupt and protect UK citizens in that sense. Where a crime is committed, either the PCeU department behind me, Charlie or ourselves will work with those agencies.

Q86 Chair: As far as al-Qaeda is concerned, is there a country that it emerges from in terms of these cyber attacks? Is there an area of the world that you look to and think, "That is the country"?

Commissioner Leppard: I am not able to answer that question; I do not have enough knowledge to. There may be others who can answer that, and I am happy to write to the Committee later if you wish.[3]

Q87 Chair: Please, that would be very helpful. One final question, Commissioner, on the issue of changing the law. If there is one thing you would like this Committee to do in its recommendations—we have just started this inquiry, obviously—what would it be? One thing to make your life easier, to make it easier for you to be able to do your job.

Commissioner Leppard: In terms of legislation, I know there is already a review of the Computer Misuse Act going on, and I think we need to look carefully at that to make sure it is fit for purpose. If I give you an example of that, the biggest threat we face in fraud is information data leaving either individuals or businesses. That is the way we are going to prevent fraud. If information is taken on a

[3] Note by witness: I have made some enquiries, with my own staff, and with other intelligence agencies, and it is clear that, due to the sensitive nature of the information, I am unable to provide a detailed written answer. The owners of this information are the Joint Terrorism Analysis Centre (JTAC), and I have been advised that the Home Affairs Select Committee has a process by which it can speak with representatives from JTAC, and that this would be the most effective rote by which to obtain this information.

USB stick out of a business, is that an offence under the Computer Misuse Act? Only if you can then prove what it is going to be used for? We need to look carefully at that against the nature of the threat we are facing, to say, "Is it still fit for purpose, or should we review it?"

Chair: We will certainly look at that. Can I take this opportunity to thank you and your team for the work that you do? In some ways it has taken us a long time to get to this inquiry, but I know you all have been working very hard on this area, and we are very grateful. Please pass on my thanks, and those of the Committee, to all the officers in your team.

In the absence of the Chair, Steve McCabe was called to the Chair.

Examination of Witnesses

Witnesses: **Detective Chief Superintendent Charlie McMurdie**, Head of the Police Central e-Crime Unit, and **Andy Archibald**, Deputy Director, Cyber and Forensics, Serious Organised Crime Agency, gave evidence.

Q88 Chair: Ms McMurdie, Mr Archibald, you are very welcome. The Chair has to go to the Liaison Committee and that is why he has had to leave. Could I begin by asking both of you how you are measuring whether or not skill levels are improving in terms of tackling this problem?

DCS McMurdie: Do you want me to start, Chair? I am Charlie McMurdie, Head of the Police Central e-Crime Unit, and also responsible for the National e-Crime Programme Delivery Team, which is the piece of business that looks at skilling up law enforcement capability. One of those programmes is to improve mainstream law enforcement cyber capability. In relation to the current skill set, we conducted a training needs analysis, looking at the requirement within law enforcement. Part of that ties in with the strategic policing requirement, which has been ongoing. That now includes a cyber aspect to that requirement among forces.

To be fair, I think we found there was a particular dearth in cyber capability currently within law enforcement, and that cyber or the use of technology is an integral part to virtually every aspect of our policing response. With that in mind, a number of programmes were initiated. If I look at those in two different camps: one was a large piece of work with Skills for Justice to map out the competencies and the national occupational standards that law enforcement should have around cyber capability.

The other piece of work that we are doing is to build and embed cyber training programmes within all the current mainstream police training courses in forces. From day one, when you join as a police officer, you will have a cyber component. Those courses are ongoing. They are being built, and we are looking at the first two main courses being rolled out in March next year that will focus on primarily open-source intelligence, but also the training course and awareness package for senior officers. The other courses are being built as we speak to go into the investigation process.

Q89 Chair: Thank you. Mr Archibald?

Andy Archibald: At the Serious Organised Crime Agency, we have a similar process in place at the minute. The challenge is very much that we have an existing workforce and investigators whose skills are very much in investigating in a traditional sense. There have been changes in the use of the internet in recent years, and as that has accelerated the skill sets to carry out investigations are very different, so we recognise that and we are addressing that in a range of ways. Initially, there is a basic foundation level of training required for all staff. We are accommodating that through some e-learning, which is accompanied by doing some testing of the learning to ensure that some of the messages have got through.

However, we recognise that different levels of skills will be required, to investigate from a foundation level to a cadre of staff who have more advanced skills and more capability, so we are focusing on a smaller number who have some greater skills in this area. Lastly, to develop or to identify some people with a particular aptitude for developing skills in this area to quite an advanced stage, so we have three levels there. We are also working with partner agencies. We have gone through some of this transition, particularly around GCHQ. We are listening to their experiences, learning from what they have gone through, and we are about to get some support from them in relation to some of the more technical aspects about how we also incorporate that into our training.

Q90 Chair: Thank you. What of the future? Can we anticipate something like the equivalent of a digital scenes of crime officer?

DCS McMurdie: I think that is a real opportunity, and that is another area that we are doing some work around to skill up front-line officers around search, seizure and retrieval of digital material. That is one of the competencies and one of the training packages that we are building. That obviously ties in with enabling those staff, not with just the right knowledge, but with the right tools to ensure that we are doing a proportionate seizure when they go out to these investigations, reducing the amount of material that we are bringing in. We are looking at the opportunity for bespoke—as we use at the moment—scenes of crimes officers, so a higher level of search and seizure capability from that front-line member of staff.

Chair: Thank you.

Andy Archibald: If I could add, likewise we have identified within our organisation a number of individuals with particular skills and trained them as digital forensics officers, so in terms of the seizure and the initial forensic examination, they are skilled and have developed skills in that area. Equally, there is a saving in terms of how we secure those services. We have previously outsourced some of that work. We are now able to bring that in-house, and we have seen some successes as a result of doing that internally, rather than outsourcing.

Q91 Dr Huppert: International co-operation is a key part of all this, and presumably you both have key operational relationships with European counterparts, for example. To what extent are those underpinned by the existing EU justice and home affairs measures, and which ones are you most reliant on? Whichever of you wishes to answer.

Andy Archibald: In relation to the threat that we face from cyber crime, clearly it is a global threat and international partnerships are pivotal. We have relationships in a number of areas internationally—with Interpol, with Europol, with the Commonwealth Cyber Initiative—and we have liaison officers in some key locations overseas.

In relation to the EU, we have a member of staff with a cyber skill background embedded in the development of the European Cybercrime Centre, which will go live in January. We want to influence the direction and the vision for that unit to ensure it complements the UK approach. We have someone there and we want to ensure that those countries that would benefit from some capacity building—I do not know if I am heading in the right direction with this.

Q92 Dr Huppert: As you will know, the Government is considering whether to opt out of all of the Justice and Home Affairs measures. I think there are 134 of them. It would be interesting to know which ones you make use of and would want to see us stay within.

Andy Archibald: We make use of Europol and we make use of Eurojust. I think the issue of—

Q93 Dr Huppert: Are those the only ones?

Andy Archibald: In terms of cyber, those are the main ones that certainly we make use of at the minute. We have quite an extensive international network. In terms of Europol, the Euro Cybercrime Unit and Eurojust are particular initiatives that we are involved in and are engaged with on a frequent basis, and we have staff there to influence that.

Q94 Dr Huppert: Detective Superintendent?

DCS McMurdie: From our perspective, we do a load of fast-time international working operationally, but then we have the strategic sharing and engagement that takes place. From our perspective, a lot of our joint operations that we have currently running with numerous countries or working together are funded under the JIT programme, and a lot of the work around research and data sharing and co-ordination of international investigations is managed and funded within Europol, so there is a potential impact that we would see there.

Q95 Dr Huppert: I would be grateful if you could write with a full list of any others that you do use, even occasionally. You do not have to list them all now, but I would be grateful if you could do that.

Can I also just ask about cloud computing services? That is posing a number of new challenges. How do you interact with the various cloud computing services, particularly the ones based overseas? Do you work through the providers? Do you work through UK courts or overseas courts? What are your routes?

DCS McMurdie: All the above. Every investigation that we touch has either suspects, infrastructure or victims, somewhere in the world or everywhere in the world. The opportunity to capture fast-time, network traffic, attacks, victim data off cloud services, wherever those servers may be, anywhere in the world.

Normally the way that we will work that would be with parallel investigations, fast-time setting up, wherever the actual data or the server manages to exist. We will run a parallel investigation with that country, get the data preservation in place, share fast-time intelligence and then follow up through the MLAT process. One of the issues around that is the timeliness of the response and the volumes of data that we are looking for, and then the legislation for that country to be able to approach the service provider to get the data on our behalf or for them to progress that.

Q96 Dr Huppert: Do you find the MLAT process satisfactory, or does it need to be improved?

Andy Archibald: It is very slow, and often, as Charlie described, the police response and engagement bilaterally is much more efficient and faster.

A couple of points around that, if I may, that I think would help. In terms of securing that information when it is cloud computing, we use the existing legislation that serves the Serious Organised Crime and Police Act, and we can go through the process to secure that information there. Where MLAT exists in terms of an evidential chain, it is right that we can use that. Of course there are hard-to-reach countries and we do not have those arrangements there. That makes it more challenging with a country with whom we do not have those arrangements, and often we will find that it is those countries where we have to try to penetrate to get the information.

Q97 Dr Huppert: We have MLATs with most countries, I believe.

Andy Archibald: Most, yes.

Q98 Dr Huppert: So there is just a small list of them that are particularly problematic.

DCS McMurdie: The issue with the MLAT is it is extremely slow; we are talking about months to obtain that data. We cannot wait months if somebody is under attack or that data has been compromised and is being used for mass fraud, for example. Also, the MLAT process for mainstream police investigations, looking away from pure cyber, whether it is online bullying, whether it is the use of technology to commit any type of offence, low-level type of offence, that data may sit anywhere in the world. Local forces do not have the resources to go through the MLAT process, and certainly the Crown Prosecution Service does not have the resources to deal with that volume of requests.

Q99 Dr Huppert: It sounds like the MLAT process could be tweaked. Are there any other key challenges you have with operating with overseas counterparts? Are there any other suggestions on how to overcome those? If not, that is—

Andy Archibald: We are developing our approach internationally. It is a real challenge because of the nature of this particular threat. Those relationships have to be worked at and worked at hard. We need to identify those countries that have the greatest impact on the UK, and how we can leverage some assistance or some co-operation from them. That is about identifying where we can put our resources to achieve that.

For example, in the earlier session, you had mention of the US experience, and certainly some of the work around academia, around partnership working with industry, around law enforcement all coming together, there are some very good and well developed examples there, which we are also part of. It is about internationally identifying where our key relationships are, have we got those relationships right and are they in the right place and, equally, is there the opportunity, perhaps, to share some capability with other countries in this particular area?

DCS McMurdie: I certainly echo those comments, but we have two main issues. The UK we can make as safe and secure as we possibly can. We can have great legislation here. The cyber criminals know they will go to the weakest country, the hardest to reach country, and they will use its infrastructure or commit their attacks from there, so we keep chasing our tail to a certain degree around that. We have seen that with a lot of the internet governance work, with sites being hosted in hard-to-reach countries that we cannot have an impact on.

The other aspect that we have to respond to is where we are being attacked in the UK from systems, infrastructure coming through proxies, potentially. Quite often we do not know where that attack is emanating from within the time-critical period, and the ability to reach out to wherever that attack may come from and take action is not covered by UK legislation and UK powers. There are some issues around that.

Q100 Karl Turner: We hear that criminals are increasingly using social networking sites to target potential victims of online scams. I wonder whether your observations support that assertion.

DCS McMurdie: Twofold, without going into too much of our operational tactics that we use in investigations, but criminals more often than not also have a social network footprint that is quite useful sometimes when we are conducting an investigation. Yes, we have seen social networks being used as per phishing-type scams. So dissemination of the scam-type email, as well as bespoke, looking at individuals' open-source footprint to target them specifically, particularly where you are trying to get an inroad into an organisation or use that intelligence to corrupt individuals or harness vulnerabilities that may exist. It is used in a number of ways, to be honest.

Andy Archibald: The other point to make around that is that there are well known social networking sites that we will all be familiar with, but internationally there are a considerable amount of social networking sites. We have evidence and have seen those for sale on criminal forums, so you would buy a social networking site that you could then restrict access to and use that. Equally, in terms of social network sites, we have seen some online chat rooms; again, access to those chat rooms is restricted. Malware and other tools and techniques, which they can sell and market to have cyber attacks, are being dealt with and traded.

Q101 Karl Turner: Do you think there should be stronger requirements on social networking sites about storing information and sharing personal data?

DCS McMurdie: There is a real opportunity, as you have just heard, about public awareness with that. There is freedom of speech, and people put all sorts of information on the internet without realising how vulnerable that makes them. Our information is out there on 500 to 600 different databases at any one time, and the criminal groups run automated programmes harnessing all that data around us, day in, day out, and then they will utilise it to their advantage. There is a real prevention opportunity. There are data sharing issues around obtaining the data when it has been compromised from some of those network providers and social networking sites. More often than not, a lot of them exist over in America, and how we obtain that data back. I think we need a balance between awareness and some sort of guidance about what personal data should or should not be retained about individuals.

Q102 Karl Turner: Talking of public awareness, where should the spend go? Should it be on public awareness campaigns or on law enforcement?

DCS McMurdie: We talk about prevention, and most people tend to think Action Fraud, Get Safe Online, the public awareness piece, which does need doing, and is very important. A lot of people will not tend to look at that sort of advice until they have fallen foul, and that is human nature. There is an opportunity to increase that public prevention with perhaps tactical engagement, so more physical interaction.

Part of the training programme that we are doing is skilling up prevention officers to give individuals that face-to-face prevention messaging, but the prevention work that we tend to do, because of our role remit, is to go after the guys that are harvesting hundreds of thousands of identities. We then would call that prevention in getting those identities, disseminating them among industries to prevent them being utilised. That is a prevention, and that is something that we capture our performance around.

There is also, with that, a responsibility for who will take those hundreds of thousands of identities and do the preventative piece of work, to tell that individual, "Your computer is potentially compromised. Your financial identity is in the hands of that criminal group" to stop it being used. We currently share all that data with the UK Payments Association, so the UK banks, and we share it with the ISPs, but where we are dealing with thousands and thousands of identities we cannot go after each of those victims, so there is a victim care issue there as well.

Andy Archibald: I do not think it is an either/or. In terms of the response to cyber crime, there are a range of things and a range of opportunities for us to have an impact. Prevention and public awareness is a key aspect of that. The Commissioner in his previous evidence referred to that as well. Get Safe Online is one example of that. The work that they are pioneering in terms of increasing public awareness, ensuring that members of the public and society are aware of anti-virus and how to protect themselves is a really, really important message, in terms of both reducing the threat and managing the threat.

A number of figures are quoted, but about 80% of attacks could be prevented if individuals or small businesses had protected themselves and taken advantage of anti-virus software. There is an education we have to go through, and I think we need to ensure that we invest the appropriate effort there. The challenge for us is: how do you measure what you have prevented, if we have done some preventative activity? I chair the steering group for Get Safe Online, and that is the challenge that I have put out to that group. If we are going to invest resources and money here, we need to be clear about the benefit and the success of that campaign.

Q103 Mr Winnick: The Police Central e-Crime Unit, which you head, reported that it has prevented—and I give the figure; I have it in front of me—£538 million of harm since last November. If that is not spin, and I would not for one moment dream that it could possibly be, how is it calculated?

DCS McMurdie: There is a bit of a formula behind it, sir, and the issue is how we capture the harm around the work that we are undertaking and the harm that we are preventing.

Q104 Mr Winnick: The precise sum?

DCS McMurdie: That precise sum, which has now increased, and we look at the ratio of investment, so how much it costs me to fund that operation versus how much harm we prevent—so, how many of those identities that have been stolen, and how much fraud they would have facilitated over a period of time. The harm formula was put together with our performance team within the Metropolitan Police, with the assistance of Professor Levy and PricewaterhouseCoopers, some time ago, and then subjected to a number of challenge panels, including the Home Office and the Audit Office. It is a fairly complex process to look at the costs that different companies suffer.

We tend to very much underestimate the figures when we look at data that has been stolen that could be used for fraudulent purposes, because you cannot assume that all that data would successfully perpetrate that fraud. Likewise, we do not tend to use the victim figure because, with a lot of the victims, there is a notional figure for how much harm and how much it costs that victim to sort out their accounts or sort out their bank accounts or that payment that has not gone through. We tend not to use that as well, because a lot of the victims that have had their financial data compromised are not necessarily aware of that fact, and that is resolved by the banks.

All our figures—and I have the latest harm reports here for the next six months—are calculated using the same formula. What is really useful is the ratio, whether people may dispute the figures, of how much fraud would be perpetrated with an identity. The ratio of return on investment is steadily increasing, so the performance of my unit, whichever formula, or sticking to that same formula, is substantially increasing. I would put that down to our building better relationships within industry and academia, who are working with us every time we take these investigations on.

An example of that is the work that we are doing with the Virtual Task Force, so all the banks now work hand-in-hand with my team and it costs me substantially less to take on that investigation and run that at a very fast pace. Whereas historically it might have taken me six, seven or eight months to conduct that investigation, I can now do that in partnership with the banks within a number of weeks, so it is cheaper.

Q105 Mr Winnick: So it is a complex calculation, at the best of times?

DCS McMurdie: It is slightly complex, but I have an explanation that I can certainly send in to you.

Q106 Mr Winnick: I am sure the Chair would agree that would be very useful. I mentioned the figure of £538 million, which you have reported, and you said it has increased. What is the latest?

DCS McMurdie: £797 million within 18 months.

Q107 Mr Winnick: Total, in all?

DCS McMurdie: That is how much harm my unit has prevented.

Q108 Mr Winnick: It has more or less doubled from November last?

DCS McMurdie: No, we were at £538 million, I believe. It has gone up, perhaps not the same increment, but we have had to back-burner some cases because of the Olympics response that we have put in place.

Q109 Mr Winnick: By a third, perhaps; a quarter to a third. I have not done the arithmetic. How far does SOCA differ from the analysis?

Andy Archibald: We have a range of measures in terms of how we measure how successful we are being, and Charlie has emphasised the importance of arrests in that in particular; it is vitally important in terms of public confidence and deterrent in the UK that we make arrests.

The reality is that being successful in cyber crime involves much more than arrests. We have heard about prevention and about having public awareness, but equally the threat that we face is international. While the victims may be in the UK, those who are perpetrating the offence may be in one part of the world, those who have produced the malware will be in another part, and the financial transactions could be in another country entirely.

In terms of arrests and disruptions, we do rely—in terms of having a real impact on cyber crime—on the co-operation of a range of different partners and countries. If we continually arrest in the UK, for the reasons I have identified, that is part of the solution. What we really want to see, to have an impact, is those that are producing the malware, hosting the criminal forums internationally and laundering the money—those are the people that we need to target to have the greatest impact.

We measure some of those things in terms of how we share intelligence and intelligence packages with colleagues internationally, and how we then track what they are going to do with that intelligence and the difference it makes. We have some way to go in terms of the UK and the National Crime Agency, National Cybercrime Unit, coming up with a measurement, a metric and a narrative that describes how successful we are. I think it is a range of things, all the way from prevention, awareness, arrests in the UK, and arrests and targeting internationally with partners.

Q110 Mr Winnick: Thank you. Just one question. How many are in your unit, the personnel?

DCS McMurdie: Within my unit, sir?

Mr Winnick: Yes.

DCS McMurdie: We have recently grown from around 32 or 33 staff, we now have an establishment of 107 police officers, police staff. That includes three regional hubs, where we fund three staff in each of those hubs in the north-west. In addition to that, we have a number of special constables and members of industry that come in and assist us. We have gone through substantial growth as a result of the spending review last year. We have increased by 70-odd staff.

Q111 Mr Winnick: The permanent staff, apart from what you have said, people coming in?

DCS McMurdie: About 107 to 108. That includes the team that delivers on those national programmes of work as well.

Mr Winnick: Thank you very much.

Q112 Karl Turner: I think you said, Superintendent, that in your view judges are passing down lenient sentences to cyber criminals—sentences that do not really reflect the harm that that criminality causes. What do you think that is down to? Do you think it is anything to do with the difficulty of the victims giving evidence as to the degree of harm that has caused to them? What else might it be?

DCS McMurdie: A number of issues. It is very difficult to put a figure on potentially thousands of victims that have been compromised and evidence how much harm that has caused. This is an age-old problem.

We had a case at court last week. Potentially, several hundred victims had been attacked, and not all of those victims are prepared to stand up and evidence that fact. It is also difficult for judges, perhaps, when they are faced with individuals who tend to be fairly young, quite often, with no previous convictions. They have committed an offence over the internet against a big banking company or whatever the business may be that has suffered some sort of loss.

With fraud, you can see the financial amount that has taken place. I think there is work to be done by law enforcement to capture the loss and the harm, the loss of those facilities in being able to trade. How much harm does that cause? To put that in front of the judge, to enable the judge to get a better picture and sentence appropriately.

Chair: Ms McMurdie, Mr Archibald, thank you very much.

Examination of Witnesses

Witnesses: **Professor Peter Sommer** and **Professor Ross Anderson** gave evidence.

Q113 Chair: Professor Anderson, you said that one of the problems for policymakers is to understand the scale of e-crime and its costs. What are the main difficulties in establishing accurate measures?

Professor Sommer: Defining what you are trying to measure. Most of the—

Chair: No, I am asking Professor Anderson first, sorry. I will come to you in a second.

Professor Sommer: Sorry.

Professor Anderson: I would agree that measurement is an issue, and the British Government, the European Government and the American Government tend to use different measures. We produced a report on the costs of cyber crime, to which I drew the Committee's attention, where we dealt with this issue by simply setting out separate categories. We have a category for those things that are indubitably cyber crime because they did not exist before the internet—things like fake AV software.

There is a category for crimes that existed before but whose modus operandi has changed completely, such as payment card fraud and much of banking fraud. Then there is a third category for frauds that have been defined to be cyber crimes because they are done online, such as tax fraud and welfare fraud. All VAT returns are now filed electronically, so if you have a carousel fraud, that is by definition now cyber crime, although the mechanisms used by people to do that are essentially no different than they were five years ago when they were all on paper. The robust way to deal with this, I think, is to just look at the categories separately.

Q114 Chair: Thank you. Professor Sommer, you were about to comment.

Professor Sommer: My apologies for interrupting prematurely. Most of these things can be defined in a number of different ways. Nearly all the frauds are going to be regarded as offences under the Fraud Act 2006, which was specifically designed to cover the e-dimension. Prior to the Fraud Act 2006, there was an issue as to whether you could have the deception of a machine—in other words, a computer—and that overcame that problem, and there are lots of useful categories within that.

Some of the other types of activity are clearly going to be offences against children. In all the estimates that people have been making about levels of harm, nobody has been talking about children, although in fact your first session this afternoon was all about children. I do not have the faintest idea how you are going to measure the harm to a child, even one whose photograph has been put up on to the internet and is there for all time. A lot of the figures end up being rather fanciful.

I have been listening very carefully to Charlie McMurdie's explanations of what she meant by harm and although I am a great fan of her work, I have always had great difficulty in understanding what this harm factor was, other than as the means of persuading people to fund her work. It does seem to me that there is an overall problem in Whitehall that, unless you can put figures on to something, the problem does not exist, and if the figures do not exist then you invent them.

I suppose an overwhelming argument of that is a report produced by Detica on the cost of cyber crime, which managed to exclude any reference to children, any reference to the effects of malware, but included industrial espionage, which happens not to be a crime in this country, even though we know it causes potentially a great deal of harm. How they managed to get precise figures on an industry-by-industry basis of the amount of losses incurred as a result of industrial espionage really beats me.

One of the things I would suggest to the Committee is that perhaps the most important statistic of all is to look at the level of computer ownership and, consequently, the level of computer use in the country. The figures from the Office for National Statistics and Ofcom are almost identical. We are now well past the three-quarters mark in terms of individual PC ownership within the home. They are all typically going to be connected permanently to the internet via broadband. My guess is that after next Christmas when lots of people will have bought tablets, those figures will have gone up enormously. To take the matter even further, although I entirely recognise why the Committee is looking at e-crime, perhaps we can no longer make the separation between crime and e-crime, and the fact that we are trying to do so, other than looking at issues of how do we resource and how do we split up the various entities that are addressing it, trying to produce overall statistics may not be terribly helpful in the end.

Chair: That is very helpful, coming from you, because it takes us on a different track.

Q115 Dr Huppert: It is a pleasure to see both of you again. I think I have detected scepticism about Detica and Home Office figures before, in a range of contexts. Can I firstly ask about digital forensic capability within the police force as a whole? What level do you think that is at, and how could it be improved?

Professor Sommer: It is very patchy. As I think you know, I am a part-time academic. Most of my income comes from acting as an expert witness, and I specialise in digital forensics. When I say "patchy", I do not mean to say it is bad. It means that there are patches of astonishing excellence. They are often at relatively low rank levels in the police. They are constables, they are sergeants, but you will find a number of them have Master's degrees. Having had to examine some of those dissertations, they are a very high level and they are internationally regarded as such.

Once you get away from those enthusiastic specialists, once you get away from what you will find in the elite teams of the sort that you have heard from SOCA and PCeU, then it gets really pretty bad. One of the problems at the moment is that the police are trying to economise to meet the 20% reduction target. Then permanent staff—perhaps civilians—are being let go, and resource is being made to the private sector.

There is a particular trap I want to draw the attention of the Committee to. Competitive tendering for outside forensic work sounds a very good idea, but in digital forensics what happens is that you are not just sending something away and saying, "Do you have a match for this DNA? Do you have a match for this fingerprint?" Most digital forensics is about reconstructing events. So the digital forensics specialists, whether they are private sector, whether they are police, need to work together with the investigating officer. That happens in the elite groups. In my experience, it happens really increasingly rarely in the lower levels of ordinary crime, where digital evidence is important.

Q116 Dr Huppert: Just to be clear, in the areas where you say it is bad, is it that digital forensics are not done, or that they are done incorrectly?

Professor Sommer: The problem is that if you have competitive tendering, it rather assumes that the tender is perfectly framed so that people know what to respond to. If the mainstreaming process of which Charlie McMurdie talked about, which I think is very important, is imperfect, then what they are asking the tenderer to do is probably malformed. If you are squeezing them on price, there is no incentive for them to go back and say, "Excuse me, you are asking the wrong question", so they just deliver on what they are being asked to do. As a result, lots of things get missed, and may only occur, may only arise, if there is then a strong defence where questions are being asked.

Q117 Dr Huppert: I will bring Professor Anderson in in a second. But can I just be clear—do you think there are any cases where it is not that things are missed, but things are inaccurately found?

Professor Sommer: I do not think I have a universal knowledge. My worry is much more things that are missed, rather than incorrect conclusions being found.

Q118 Dr Huppert: Professor Anderson?

Professor Anderson: I would agree that forensics tend to be patchy. There have been many cases of things missed, one or two notorious cases of wrong conclusions being drawn, although that tends to have been some years ago, as things are getting better.

Generally, the problem is that, as computers and communications become embedded everywhere, digital forensics then become a part of every investigation. The state of affairs is better than it was 15 years ago, when I started getting involved in policy, or 30 years ago, when I started doing this, but it still has some way to go.

Q119 Dr Huppert: What steps do you think need to be taken to improve it? What should we be recommending?

Professor Anderson: The ability to deal with digital evidence has to be integrated into the police force everywhere and at all levels. You might care to draw an analogy with the arrival of the motorcar two generations ago. It would now be unthinkable for a police officer to be unable to drive, unless they had been disabled but kept on in a back-room job, but it is perfectly thinkable to find even chief constables who would get their secretaries to deal with their e-mail.

Dr Huppert: Unlike Members of Parliament, of course.

Professor Sommer: We have heard a lot about mainstreaming, and I do not regard it as the fault of the officers you have had in front of you. This policy of mainstreaming has been around for five years, at least, to my certain knowledge, if you go and look back at some of the policy documents that have come out, and it always comes along very, very slowly. One of the other areas you need to look at probably is the capability within the Crown Prosecution Service to handle all these things. You can see the policies are there. It is just that they are not rolling out at the speed with which people are using computers. As a result, digital evidence is important.

Q120 Mr Winnick: Professor Anderson, you have of course appeared before us on previous matters in the last Parliament. I do not think events have proved you wrong by any means. You are both rather sceptical about the action being taken on e-crime, but you were present a few moments ago when the Head of the Police Central e-Crime Unit referred to the sum of money, now over £700 million—increased, as she told us, from November last year. Surely that demonstrates that it seems to be working.

Professor Anderson: What we have done in the analysis that we did for the Costs of Cyber Crime Report, which was requested by Sir Mark Welland, the Chief Scientific Officer at the MoD, after there was widespread scorn for the Detica report, was to try to unbundle things into direct and indirect costs. When you look at that, you discover that many of the costs of cyber crime are indirect costs, and I do not think that official accounting takes this into account properly.

Let me give you an example. In the year 2010, about a third of all the spam in the world was sent by one botnet, the Rustock botnet, and the owners of that botnet earned about $3.5 million from what they did. There was a colleague of mine in California who went to the trouble of tracing this with test purchases of Viagra and so on so that he could get some forensics. In broad terms, spam cost the world $1 billion, most of this falling on ISPs and on service companies like Google. If a third of those are back to the Rustock botnet, then for every $1 the bad guys made, there was $100 of costs fell on everybody else. This is very, very different from traditional fraud, such as tax fraud, where the amount that the fraudster gets away with is typically most of it, and the indirect costs, the enforcement costs and so on and so forth, are but a small proportion. So, you are dealing with an intrinsically different animal than you are with conventional fraud, and using conventional Home Office methodologies is not necessarily the best way forward.

Q121 Mr Winnick: Either Professor Sommer or Professor Anderson, as briefly as you can, what would you say the Government should be doing that it is not doing?

Professor Anderson: We should be locking up more villains. We should be putting more of the cyber budget into policing and less of it into the intelligence sphere, into cyber war, broadly defined. This Government made a very welcome increase of £640 million in the cyber security budget two years ago, but 59% of it went to GCHQ and only a few million to the police. Had I been in the room when that decision was taken, I would have argued for the police to get more at the expense of GCHQ.

Q122 Mr Winnick: Professor Sommer, more or less the same?

Professor Sommer: More or less the same. I want to add something, and I think it emerged out of your questioning. I think you were absolutely right to press everybody on public education and on prevention, because no matter how good the police are, they are only going to be able to scratch the surface, and there is a lot to be said for helping people help themselves. In addition to doing that, one of the big routes for cyber crime is the so-called botnet, when you have poorly-secured computers, so there is a public health argument as well in terms of persuading people to look after their computers.

Again, if you go back to the budget, I have been looking at this budget, and I was looking at it again last week when we had the annual report from the Minister, and I was saying, “Where is this preventative thing?” and it has all rolled into other places. It almost becomes discretionary for the police, as part of their role, how much they are going to assign to it. If one looks at the single element that is assigned to public awareness, which is Get Safe Online, their budget over four years is £395,000. That is 0.06% of the total. That seems to me to be tragically low, and I agree with Ross that taking a few million away from GCHQ, for all the good work we believe they are doing, and putting that over to public prevention would be astonishingly good value for money.

Q123 Mr Winnick: Would you, have you, or are you intending to put this in writing to the appropriate Minister?

Professor Sommer: I put it in writing, partly, to you, and I was rather hoping that, as an influential Select Committee, the Minister would see it. I have raised this with the Cabinet Office. In fact, I raised it before their first report was published. They did call a number of us in to discuss a number of the issues, and I did keep on saying, “How much are you assigning towards all of this and towards public education?” They said, “You make a very interesting point”, but when I came to look at the assignments and the final documents, I obviously was not as successful as I would have liked to have been.

Mr Winnick: The Ministers will see our report in due course, and hopefully the Home Secretary or whatever, the officials, will go through the questions and answers of sessions like this. Thank you very much indeed.

Q124 Mark Reckless: I am a little concerned about dismissing perhaps what GCHQ is doing with this money, not least because I do not have a good understanding of what that money—

Professor Sommer: I am not dismissing. They easily have the largest budget, on the basis that £650 million over four years is not going to be extended. The obvious place to look, if you are going to take money away, is the largest budget-holder.

Q125 Mark Reckless: Is it not possible that that may lead to some things that are very important not being done?

Professor Sommer: I do know a few people at GCHQ, but my overview of their general policy, I am afraid, is as opaque as almost everybody else’s who is outside that particular environment. It has always been, I think, the big problem in evaluating police cyber security policy. There were a number of discussions both before and afterwards, and I remember asking the Cabinet Office, who were disposing of the money, and alas, as with so much to do with intelligence work, you have to take it on trust and hope that the trust is justified.

Q126 Mark Reckless: But you do not take it on trust, and are confident that if that money were redeployed there would be better returns to it?

Professor Sommer: All I am saying is that, if you take an organisation that has only £100,000 a year, does not have an office, and you were to give them another £1 million, I suspect that the benefits would be rather greater than another wonderful machine to carry out surveillance by GCHQ. That would be my guess.

Q127 Mark Reckless: Thank you. Do you recommend making any changes to crime recording practice to get a more realistic or broader understanding of online crime? Would that be sensible?

Professor Anderson: This is something that we have spoken about a number of times over the years, since 2005 when the previous Government—unfortunately, in my view—decided that fraud reporting should be done to the banks, rather than to the police. This caused the fraud statistics to go down, but it opened up an even larger gap than is usually the case between the crimes reported through the police, on the one hand, and the crime levels reported through victim surveys on the other. Now, for most practical purposes, official recorded crime is useless in determining the level of fraud.

The most recent UK official figures that we have are annex 3 to the British crime survey for 2010, which suggested that, although our risk of becoming victim to a traditional acquisitive crime, such as burglary or car theft, was about 2% per annum, your risk of becoming a victim of fraud was about 5%. The only figures we have had since then was a Eurostat survey in 2011, which was conducted across the Member States of the EU, which suggested that in the UK we were in the second-worst position after Latvia.

Both the experience of crime and the fear of crime appear to be significant in this country, yet official crime statistics do not give us any pointer, at least in England. In Scotland, things are different, because there was a survey there last year that indicated that the main fear of crime north of the border is of online crime, card and online banking crime—not of violence or mayhem, despite my countrymen’s reputation for that. Very, very patchy official statistics have arisen. If you could nudge the Government towards fixing that, that would be useful.

Professor Sommer: There is another recommendation you might like to think about. If you perhaps follow my earlier remark that lots of things can be defined both as a cyber crime and as an ordinary crime, the police have systems for when a crime is reported to enter things on to a form so that they can build up statistics and they can then follow the crime up. There was some discussion a few years ago about introducing a field in that form as to whether there was digital evidence.

I do not know how matters have progressed at the moment, but that seemed to me to be an excellent idea because at very, very low cost you would be able to go back across a whole range of crimes, see where digital evidence seemed to be important and you would then be able to do resourcing. That would be without getting into statistics about whether it is a fraud or whether it is an extortion or any other sort of thing that you might call cyber crime. It seemed to me to be a low-cost solution. I know there was a proposal. I do not know where it has gone to at the moment, but I think it might be something the Committee may want to probe.

Q128 Dr Huppert: Firstly, Professor Anderson, just very quickly, you were somewhat critical of the limited amount of funding that was given to the police from the cyber security programme. How much should they be getting? Can you put a number on the size you would like to see?

Professor Anderson: I have not thought that through in concrete budgeting terms, but what is needed in operational terms is basically to train the entire UK police force to deal with digital issues competently, and to have sufficient specialist resources that we are able to go after the perpetrators of large-scale globalised petty crime. This is one of the things that is almost ignored at the moment.

Typical large-scale cyber crime might consist of somebody in Russia sending out 100 million phish and getting a few hundred respondents and defrauding each of a few thousand pounds. Each of these crimes individually falls below the radar. What we need to do, in order to have a proper determinative effect, is to consider them in total and work together with agencies in other countries where there are victims, to go after the bad guys and lock them up. That is not being done enough at the moment.

Q129 Dr Huppert: Professor Anderson, you cited, in your evidence to us, the banking regulations being the UK's biggest legislative failure in relation to tackling e-crime. How would you change that?

Professor Anderson: What I have been doing to try to change it is trying to educate people about the consequences of the regulatory failure. The problem is that in Britain, banks often find it easy to blame their customers for fraud. We have been doing this firstly through the press. There was a Channel 4 *Dispatches* programme last night, which showed that, for example, the Ombudsman was dealing with about 70 cases per day where customers did not get their money back from banks after fraud.

We have been lobbying BIS and the Bank of England about this. The problem was that the Financial Ombudsman Service considered itself to be independent, and therefore nobody wanted to touch it. The Financial Services Bill that is currently going through Parliament—or perhaps it has just gone through; I do not know—should give the FCA the power to regulate the Ombudsman Service from next year, so we will be seeing the FCA and presenting files to them of cases in which the Ombudsman has failed.

The failure is that the Ombudsman, in effect, has completely ignored the Payment Services Regulations 2009, and people going to the Ombudsman with complaints found that the responders were unaware of the existence of the regulations. The banks have therefore being treating the Payment Services Regulations as if they did not exist. There is consumer protection, which the European Parliament and this Parliament wisely enacted, but it has not had any force or effect.

Q130 Dr Huppert: One suggestion that we have had from some people is that victims who suffer personal loss should have some liability if they were negligent about their own computer security. Do you think there is any merit in approaches like this, either of you?

Professor Anderson: The banks certainly claim that they will blame people if there was gross negligence. In practice, they often blame people as a routine matter, even when it is not clear there was negligence at all. One of the things you have to be very careful about here is safe default. I am not quite as enthusiastic about public education as some other people, because of the simple fact that computers and mobile phones and social networking sites tend to ship with unsafe defaults because it is better for selling advertising.

So you have to think very, very carefully in this context: what do the equipment vendors, the service providers and so on want people to do, and what are the risks to which that exposes people? In such circumstances, you then have to ask to what extent it is reasonable, in given circumstances, for banks to impose liability on people. The problem is it is a shallow gain here. Everybody is trying to push liability on everybody else. It is even fashionable in the industry. We call it leverage. The buck has to stop somewhere, and ultimately it is down to the legislator to decide where the buck should stop.

Professor Sommer: The problem is also evidence. How do you show that something has actually happened? Most people have no idea how to even address the problem, so they are always at some considerable disadvantage, as Ross has pointed out.

Q131 Chair: Finally, gentlemen, could I ask whether you think it is possible to secure large Government databases against cyber attack?

Professor Anderson: There is a problem in that you can have security or functionality or scale. If you are a good engineer you can have any two of those, but people putting out tenders for systems in Whitehall tend to assume that getting all three is trivial.

Q132 Chair: Professor Sommer?

Professor Sommer: I think Ross has captured it. The more people that have access to a system, the more likely it is that there will be some sort of failure, even if the technical side of it is absolutely immaculate. You are right to ask the question. I am afraid it is an impossibility.

Chair: Gentlemen, can I thank you very much on behalf of the Committee for your evidence? That concludes our business for today.

Tuesday 29 January 2013

Members present:

Keith Vaz (Chair)

Mr James Clappison
Michael Ellis
Lorraine Fullbrook
Dr Julian Huppert
Bridget Phillipson
Mark Reckless
Mr David Winnick

Examination of Witnesses

Witnesses: **Tom Ironside**, Director of Business and Regulation, British Retail Consortium, and **Mike Andrews**, National E-Crime Co-ordination Manager for the National Trading Standards E-Crime Centre, gave evidence.

Q133 Chair: We have business in the House today, so I must apologise if, as is likely, in the middle of your evidence I suspend the Committee so that Members can vote. We will come back, so do not feel that we have abandoned you. As you know, the Committee is undertaking an inquiry into e-crime and clearly the views of your organisation in particular. Mike Andrews, you are the e-crime co-ordination manager for the National Trading Standards E-Crime Centre. Could you tell us something about current trends in this area? Is it on the increase at the moment?
Mike Andrews: Yes, there is certainly anecdotal evidence to support the suggestion that there is an increase in e-crime, particularly in terms of the trading standards remit, which is where we are approaching this from in terms of scams that are targeted at consumers. Some examples that we are particularly seeing are job opportunity scams, advance fee frauds, anti-virus software scams and vehicle-matching scams. What we are seeing more and more is that a lot of these scams that were done in the physical world, in terms of trading standards enforcement, are now moving more and more towards being perpetrated online, on the internet and email and technology like that to facilitate the crimes.

Q134 Chair: From where you are and from what you see, where are these scams coming from? Are they onshore, or are they coming other countries?
Mike Andrews: There is a mixture. In terms of obviously getting into trading standards, we are looking at where we can enforce UK legislation, but more and more the intelligence that we are receiving suggests that there is an increasing element of offshore criminality.

Q135 Chair: What the Committee is very interested in is the fact that certain other countries appear to be targeting the United Kingdom, partly because of our very buoyant retail market. If you look offshore, is it coming from other European countries or from beyond Europe?
Mike Andrews: It is very much a mixture. It is from other European member states; it is from former members of the eastern bloc; it is coming from the far east. It is very difficult to pinpoint specific locations because it truly is, to use a cliché, a global problem.

Q136 Chair: Mr Ironside, welcome. Your own recent survey shows losses of about £205 million?
Tom Ironside: It does.
Chair: How does that compare to other losses that are suffered by the retail industry, such as shoplifting and other crimes of that kind? Are you seeing an increase in this trend?
Tom Ironside: Yes. Our annual retail crime survey was published at the start of last week, and that showed a £1.6 billion impact on the retail sector of crimes relating to retail activities. That represents a smaller proportion of overall retail turnover than the £205 million does of the £29 billion or £30 billion that currently passes through online retailing. You can see that it is some way beyond the more general sort of tonal activity that takes place across the sector. I think that some of that is associated with the fact that it is a relatively new channel with relatively new challenges and, we think, some particular issues to be focused on from a law enforcement perspective in particular.
Chair: We will come on to some of those.

Q137 Michael Ellis: Mr Ironside, can I just ask you about two particular issues. One is proportionality. How do you approach the prosecution of offenders who may have stolen an item that in and of itself is of low value, but where the prosecution will obviously necessarily cost an awful lot more than the value of the item? There is a public interest in prosecuting those individuals, but do you have anything to say about the issue of proportionality?
Tom Ironside: I think we have a general view about proportionality, in that we see that any criminal retail activity is a matter of serious concern and should be taken seriously by all concerned. We have a broader issue in relation to e-crime in particular, which is that we think that local response, be it in terms of reporting, of investigation or of enforcement, is seen to be not ideal as it currently stands. We have questions about the extent to which local law enforcement officers are in a position to meaningfully progress cases. It is more from that perspective that we approach that question.

Q138 Michael Ellis: Can I ask you also about the increased use of mobile technology, because you have spoken about this and the challenges that the increased use of mobile technology holds for retailers? What do you perceive to be the main challenges?

Tom Ironside: From a mobile perspective, we do not see that there is a different set of criminality that accrues to mobile commerce as compared with other forms of online retail criminal activity as it currently stands. We put a lot of that down to using exactly the same sorts of measures to screen and tackle fraud within an m-commerce environment. There is an emerging expert view that the real challenge in mobile technology is the personal information that people keep on their mobiles, and that seems to be more problematic. It is more about the information that mobile phone users are choosing to store on their phones, and there is the potential for malware and other software applications to access that. But that is not a specifically retail-related issue.

Q139 Mr Winnick: Mr Andrews, you have a particular responsibility, have you not, for the protection of the public? Do you feel that sufficient protection is available for people, bearing in mind the scams that are now constantly being undertaken?

Mike Andrews: It is fair to say that in terms of legislative protection and of what criminal enforcement can be undertaken or of the civil remedies that are in place, the existing legislation is broadly adequate because it works equally well in the physical world as it would do in the virtual world in terms of e-commerce and e-crime. From that perspective, we do not really have any issues. The difficulty we have is more from the enforcement side, in particular the changes that have been put in place in terms of the Regulation of Investigatory Powers Act and plans in the draft Communications Data Bill that will potentially make it more difficult for us to tackle the problem, particularly in relation to getting communications data in relation to offending that is happening online.

Chair: Thank you. I am going to stop you there because we have to vote. We will continue with the questioning afterwards; we will not abandon you. I suspend the Committee until 4.15pm.

Sitting suspended for a Division in the House.

On resuming—

Q133 Mr Winnick: Mr Ironside, you represent of course the retailers. Retailers obviously want to make as much profit as possible. It would be odd otherwise, as you are in business to succeed and I am sure at the same time to try to be as fair as possible to your customers. Do you feel that customers have enough protection against online scams?

Tom Ironside: Consumer relationships are absolutely fundamental to the successful running of BRC member businesses. We certainly feel that the resourcing that is now being allocated to looking at online scams, rip-offs and other borderline criminal activity is absolutely right, because if consumers lose confidence in online commercial activity, then that has a knock-on effect right across the sector, we would feel. We do not have a perspective that there is insufficient resourcing currently, but we welcome the fact that this focus is emerging.

Q134 Mr Winnick: Yes. You are sitting together. I assume there is some co-ordination between the organisation Mr Andrews represents and retailers?

Tom Ironside: We were just talking about the fact that there definitely should be some co-ordination between our organisations, and we can see some strong potential in doing so. I am aware that the unit Mr Andrews is working in is relatively new, so it prevents—

Mr Winnick: At this moment there is not, but it is your intention there should be?

Tom Ironside: Indeed.

Mr Winnick: Mr Ironside, I should have thought the initiative, to a large extent, should come from your part of the affair.

Tom Ironside: We are very happy to make that connection and see whether there are ways that we can work together.

Q135 Mr Winnick: From this day onwards, so to speak. During the break when we were having a rather crucial vote, you came to the conclusions that you just told us?

Tom Ironside: There was clearly quite close alignment between the sorts of things that we were saying in our submissions, happily, and I can see that there is potential for us to work closely in the future.

Mr Winnick: Perhaps we could be kept informed of developments.

Tom Ironside: Very happy to.

Mike Andrews: Absolutely, yes.

Q136 Chair: In respect of victims of some of these crimes, recently my credit card was hacked, a PayPal account was set up in my name and money taken out of my account to pay for something. Obviously the money has been returned by the bank, but when I inquired of PayPal and others who was responsible, there did not seem to be any interest in finding out who was responsible for this; the main interest was obviously in ensuring that I was satisfied and that I had my money back. Do you think that this is a problem in dealing with online crime: nobody traces it to the very end to find out what has happened?

Mike Andrews: I think you have absolutely hit the nail on the head there. Before the suspension, one of the points I was keen to stress was that when you are dealing with the physical world it is relatively easy to identify if somebody is up to no good. It is quite easy to identify a shop or a house that you can pay a visit to in the physical world, but in the virtual world it is that much more difficult to trace where the offender is. You are relying on e-mail addresses, credit card numbers, mobile phone numbers and so on, and to trace that information is quite difficult. That is where we have serious concerns in relation to the proposed changes to allowing local authorities to have access to communications data, because clearly the access to the subscriber and usage information in relation to communications data is vital in being able to track and trace offenders who are operating in the virtual environment. Proposals to remove access to that information would have a significant detrimental impact on our ability to trace those offenders, and the example you have highlighted there is a perfect case in point.

Q137 Mr Clappison: How successful do you think Action Fraud has been at gaining recognition as a central reporting point for e-crime?
Mike Andrews: I think recently there has been a lot of publicity. I believe it was five police force areas it was initially trialled in and it is now being rolled out across the remaining police forces in the UK. We welcome the idea of having a central reporting point for all forms of fraud and obviously in particular in relation to e-crime and internet fraud. What we are slightly concerned about is how that information is then co-ordinated and disseminated to agencies like ourselves so that we can take appropriate action, because obviously we have a remit in terms of enforcing consumer protection legislation. It is vital that that information that is fed into organisations such as Action Fraud is properly co-ordinated and disseminated to agencies who can take the appropriate action. We welcome the progress that has been made, but I think it is quite clear that we need to engage closely with them to ensure that information is followed up.

Q138 Mr Clappison: On that point, do you think that current crime recording conventions give an accurate picture of the profile of e-crime? How do you think this could be improved?
Mike Andrews: It is fair to say that the current recording mechanisms probably are not adequate because you tend to find that the illicit activity would get recorded as a general fraud or a consumer protection legislation issue in terms of, for example, a trademarks offence if they were counterfeit goods. They tend to get classified under those areas, but the e-crime element is not necessarily always picked up. Therefore, it is fair to say that there is probably a large-scale under-reporting of e-crime and its true economic impact.

Q139 Chair: What kind of communication is there between banks, the law enforcement agencies and yourselves, not just yourselves as individuals, but in terms of retailers? I think you have said in the past, Mr Ironside, that there needs to be better communication between banks and card users. What kind of information would it be helpful for you to have in order to deal with this very serious problem?
Tom Ironside: There are a couple of areas in particular that we have identified where we think improvements could be made to the way in which banks communicate with retailers. When a card is flagged as lost or stolen, we find out very rapidly that that is the case and we can take action as a result. However, where fraudulent activity is undertaken, the communications links are much slower, and we think there is a clear case for that being addressed and flagged in an appropriate way so that retailers can take appropriate action at the time in question. The other issue that has been raised by members in this context is wanting to have a better or deeper understanding in relation to card-not-present transactions, where again there is an absence of depth of knowledge, which would allow retailers to respond particularly when fraud turnover threshold ratios are being approached. I think there are some quite straightforward things that would assist retailers to respond in an appropriate way.

Q140 Chair: I would have thought that the arrival of the unique personalised PIN number—presumably only people who know what their PIN number is should be able to use a credit card—would have cut down on the amount of fraud that is being committed, but it seems to have gone up.
Tom Ironside: I am absolutely sure that chip and PIN has had a significant impact in that context.
Chair: What, to make it better or worse?
Tom Ironside: It is a counter-factual case, but it has prevented fraudulent activity that would have otherwise taken place. However, it is a growing area of retail activity, so it is accompanied by criminality that sits alongside that and not all of that relates to card-not-present activity. Some of it is identification-related; some of it is refund fraud. There are all sorts of different strands to it.

Q141 Chair: But presumably, even though you might be able to stop the use of a fraudulent card, if somebody has ordered something online and purchased it, it must be very difficult to get back the product itself. You may be able to stop the use of the card. Is there any evidence to suggest that you get the product back?
Tom Ironside: I suppose it depends on the point at which the fraudulent activity is detected. There is considerable sophistication in the way that the third-party screening companies look at commercial approaches from customers. Where there are multiple uses of the same card across a range of different products, where there are a multiple uses of the same address in deliveries, then that can throw up warning signals in advance.

Q142 Lorraine Fullbrook: You have both criticised the capacity of law enforcement to respond to low-level, high-volume e-crime. Have you noticed any improvements in this area?
Tom Ironside: From our point of view, if I can respond, we have not, and I think that retailers' perspective currently is that there is a lack of confidence in the local response. I think it is understandable that at a local level you will not necessarily have the expertise or the resourcing to adequately address what can be a technologically complex and difficult area of criminality. What we would like to see—and it goes back to an earlier answer—is a very effective central reporting mechanism that allows bulk reporting because, as I was mentioning, quite often you get a linked range of, say, 200 offences, all of which relate to a single card or a single address. Expecting an individual case report for each of those is perhaps not the best way to go about things and we think there are ways to make that process as business-friendly as possible.
Mike Andrews: I echo that and I would like to think that the advent of Action Fraud as a central reporting centre would help to collate that intelligence so you

can identify these patterns. The problem is that, from a trading standards perspective, you may get a number of different reports that are reported to individual local authorities, but then trying to collate that into this issue of low value but high volume is very much an area where we have a key remit to enforce that.

Q143 Lorraine Fullbrook: Mr Andrews, you have said that the recent changes to RIPA have impaired the ability of trading standards officers to investigate online offences. What is your estimate of the proportion of your investigations that have been adversely affected by the changes?
Mike Andrews: The changes are very recent. The changes in terms of having judicial approval for RIPA authorisations only came into effect in November, so it is quite difficult to quantify that at the moment, but I am aware that the Local Government Association is in the process of collating figures from local authorities across the UK to try to quantify the problem that this is causing. What is more concerning is not so much the changes to RIPA in terms of doing directed surveillance. I go back to my earlier point: the key changes that are planned are in relation to access to communications data, because that is fundamental to allowing us to track and trace offences that are occurring online. Removal of our ability to access that data will severely hinder the work that we can do.

Q144 Lorraine Fullbrook: You see that currently as an obstacle?
Mike Andrews: Yes.
Lorraine Fullbrook: What other obstacles would trading standards encounter when investigating online crime?
Mike Andrews: One of the key areas is the cross-border nature of e-crime, and that is why the unit that I am responsible for has been set up. Trading standards obviously operates at a local level through local government, but clearly e-crime is not confined to any one local authority area. Hence we have set up a national unit to tackle that problem, but at the same time we rely on colleagues in local authority departments to support us in that endeavour. Clearly government resources are under severe pressure in terms of budget cuts and e-crime is not always seen as a priority by council members and local politicians. Trying to get that engagement and work with local authorities is quite difficult in these times of austerity, so that is a key barrier for us. Further to that is also the very nature of e-crime. It is quite a complex, time-consuming area of criminality to investigate, hence the resources required to do so are quite—

Q145 Chair: Finally from me, DAC Leppard from the City of London Police said that we are not winning the war against online crime, and only last week a number of people who had anonymously hacked into PayPal had been given sentences of between seven months and 18 months, even though they had been responsible for fraud of £3.5 million, and one would believe that if you had robbed a bank, you would get a bigger sentence than that. Are you concerned, first, about the level of sentences of those who are involved in e-crime? Secondly, are we winning or are we losing the war against e-crime? Mr Andrews first, and then Mr Ironside.
Mike Andrews: I think the case you have highlighted there is a perfect example in that perhaps the sentencing is not adequate, because, as you have pointed out, if somebody walked into a bank with a sawn-off shotgun, they would have probably received a sentence significantly longer than that. Are we winning the war? Again, it goes back to the ability to properly quantify e-crime and the economic impact. I do not think we can fully quantify that at this stage, but it is certainly true that unfortunately the cyber-criminals are generally one, two or even three steps ahead of law enforcement in terms of their ingenuity and the methods that they have to hide behind the anonymity of the internet, and it makes it all the more difficult for us to track and trace those sorts of offenders.
Tom Ironside: From our perspective, if you do not have meaningful and effective enforcement, i.e. if you do not take appropriate action once criminality has been identified and see the punishment that flows through from that, then that obviously causes some extremely difficult messaging and potentially encourages additional criminality. Looking at incidence of e-crime, I think investment by businesses is successfully screening out lots of criminal activity. We can see potential in a move to a central reporting mechanism, but what we really need to see is that central reporting mechanism working effectively and delivering the investigations and enforcement that flow out of that. That is something for the future rather than something that is here already.
Chair: Mr Andrews and Mr Ironside, thank you very much for coming. I am sorry it has been a disjointed session, but we are most grateful to you for coming, and there must be other information that you feel would be of help to us. If there is, please do not hesitate to write to us. We are very pleased that you have had the opportunity to bond during the important vote on boundaries in answer to Mr Winnick's question.

Tuesday 26 February 2013

Members present:

Keith Vaz (Chair)

Mr James Clappison
Michael Ellis
Steve McCabe
Bridget Phillipson
Mark Reckless
Chris Ruane
Mr David Winnick

Examination of Witnesses

Witnesses: **Sarah Hunter**, Head of UK Public Policy, Google, **Simon Milner**, Director of Policy, UK and Ireland, Facebook, and **Sinéad McSweeney**, Director of Public Policy EMEA, Twitter, gave evidence.

Q146 Chair: The Committee is now in session. I refer all those present to the Register of Members' Interests, where the interests of Members of this Committee are noted. This is a session of the Committee's inquiry into e-crime, and at the end of this session we will go into private session to consider other business. Could I welcome Simon Milner, Sarah Hunter and Sinéad McSweeney? Thank you very much for coming to give evidence.

It has been a long, hard struggle for this Committee to try to get your companies to appear before us. As you know, we were very keen to hear evidence from the people responsible for security, because of course this inquiry is into e-crime, but that I understand was not possible. Is that correct, Ms Hunter?

Sarah Hunter: We are happy to provide further evidence in private with our security leads, and I am happy to talk about the broader policy issues today.

Q147 Chair: Yes, we did want to do this, but I think there was a problem with getting them because they are all in America. Are your security people in America, Mr Milner?

Simon Milner: Yes, the people who lead for us on law enforcement liaison are in the US.

Q148 Chair: Yours, Ms Hunter, also in America?

Sarah Hunter: That is right, yes.

Q149 Chair: Yours, Ms McSweeney, also in America?

Sinéad McSweeney: Yes, that is correct.

Q150 Chair: Therefore, the operation of Google, Facebook and Twitter in the UK is quite limited, is that correct? How many people do you have working here, Mr Milner?

Simon Milner: We have around 130 people working in the UK, predominantly in our sales operation, although we also established an engineering group in October last year, so that is a growing part of our operation in London.

Q151 Chair: I am going to start with a question that was raised by the judge in the Birmingham case last week concerning the use of the internet by organisations and individuals who are perpetrating attacks and verbal incitement of attacks against individuals in the state. I went on YouTube this morning, which of course is owned by Google, and I noted the fact that the preachings of Anwar al-Aulaqi, who was head of al-Qaeda in the South Arabian Peninsula, are still on YouTube, and those addresses, some of which could be seen to be inciting religious and racial hatred, are still on YouTube. Why is it that they are retained on there, given the record of that individual?

Sarah Hunter: It is a good chance to talk about this. Thank you for bringing it up. It is worth saying from the outset that we in no way condone the use of YouTube for terrorist content, and to that end we have very, very strict community guidelines on YouTube that go way beyond the law. For example, it is not allowed on YouTube to post content that is inciting violence; it is not allowed to post content that is hate speech. When a user flags to us that there is content up on there that is breaking those guidelines, we review that content and we take it down, and these flags get reviewed within an hour, so it is a very quick process.

Q152 Chair: How many people do you have doing that?

Sarah Hunter: We have many people. They are spread across the globe so that we can make sure that whatever time zone you are in, when you flag something, it is immediately looked at. They are spread across a number of different locations.

Q153 Chair: But bearing in mind that this particular individual has been described as, when he was alive, number three to Osama bin Laden, and that he headed the organisation in the South Arabian Peninsula that was responsible for many deaths, why is his content still on YouTube?

Sarah Hunter: When content gets flagged to us as having broken our guidelines, these people review it, and they look at every single one and they look at it very carefully, and they look at the context. They look at what is actually being said, and they look at whether it is indeed inciting violence.

Q154 Chair: So you have looked at it? Somebody has looked at all these references to Anwar al-Aulaqi?

Sarah Hunter: If someone has flagged it to us, yes.

Q155 Chair: "Flagging" means what? Can you tell us?

Sarah Hunter: When you go on to YouTube and you look at a video, in the bottom right-hand side there is a little flag sign, and you can click on that and it says, "Do you want to report this content?" and you have to click on the reason why, and that is what flagging means.

Q156 Chair: Sure, and this has been done in this particular case?
Sarah Hunter: I don't know if it has been done in every single video. Anyone could do it. I could do it; you could do it.

Q157 Chair: No, I know, but I am referring to it specifically, and if you do not know the content—I am very happy to accept that you do not know the content, but this is the content of speeches by Anwar al-Aulaqi, who was wanted for a number of criminal activities and whose preachings were noted by the judge in the bombing trial of last week in Birmingham. Are you familiar with what I am talking about?
Sarah Hunter: I have seen some of this content on YouTube.
Chair: You have?
Sarah Hunter: I have seen some of his content on YouTube, yes.

Q158 Chair: You are satisfied that this content is not content that YouTube is concerned about and that ought to be taken down? Somebody has looked at this content, they are very happy that it comes within your guidelines and it therefore remains on the internet? You are happy with that, are you?
Sarah Hunter: I haven't personally looked at all of this content, and it is just worth remembering the scale of content on YouTube. There are 72 hours of content uploaded on to YouTube every single minute of the day, so it is just physically not possible for us to look at every single video that gets uploaded. We rely on our users, and there are hundreds of millions of people across the world looking at YouTube all the time. When they tell us there is content that breaks the guidelines, that is when our team kicks in, reviews it and removes it.

Q159 Chair: You will then look at it. As a matter of policy, can you just tell me how many of these videos you have taken down as a result of somebody alleging a criminal act is being incited and therefore you have had to remove those videos?
Sarah Hunter: I don't think we have specific numbers of how many broadly are flagged and then removed. We have numbers of how many—

Q160 Chair: You have no indication of how many people have complained or flagged? An internet company like yours, with so many databases, so many experts, will not know how many people have flagged a particular video?
Sarah Hunter: We probably would internally within the YouTube removals team, but I don't personally have that number here, no.

Q161 Chair: No. So, you would know? You do have that information?
Sarah Hunter: When a video gets flagged, yes.

Q162 Chair: Yes, and you would also have the information of how many of these videos have been taken down?
Sarah Hunter: Of the ones that have been flagged, yes.

Q163 Chair: Yes, and how many are there?
Sarah Hunter: I couldn't tell you now. I can probably ask.

Q164 Chair: Would you write to the Committee?
Sarah Hunter: Absolutely. I will ask.
Chair: We are very happy if this needs to be in private. I do not see why it should be, because this is just a matter of fact. If you could write to us and tell us the figures as to how many of these videos have been flagged and how many have been taken down—
Sarah Hunter: Absolutely.

Q165 Mr Winnick: Following what the Chair has just said, recognising again the extent of the communications involved—some totally unknown, obviously, up to 10 to 15 years ago—it is not simply the rantings of the cleric mentioned by the Chair, but other incitements to hate crimes, certainly against Muslims, anti-Semitism and the rest. You say matters are flagged up when complaints are made. My question is, before complaints are made, what sort of control is there to try to ensure that hate crimes—incitement against people because of their racial origin, religion or sexuality—do not go on?
Sarah Hunter: Because of the scale of the amount of content that gets uploaded on to YouTube, we do not have a way of reviewing it in advance of its being posted, but it is an amazingly effective system, this flagging system. Because we have hundreds of millions of people looking at YouTube all the time, things get flagged very, very quickly, so if there is content that the users, the real people using YouTube, believe is breaking our hate speech rules, for example, it gets reviewed and taken down within an hour.

Q166 Mr Winnick: There is all the difference, obviously, between that and a newspaper, which would be very anxious, if it was responsible, regardless of its political stand, not to include any item that incited hatred. In this form of technology, that is not possible, or does that—
Sarah Hunter: Yes. YouTube is a very different platform to a website that a newspaper publishes.
Mr Winnick: I understand.
Sarah Hunter: We do not choose what content gets put up on there, and that is one of the great things about this platform—that anyone can put content up on YouTube and express a view or launch a band or put a film up. It is an incredibly open system, and it means that people have an opportunity to express themselves in a way they never had before. If you look at the use of YouTube, for example, in the Middle East, it has been an amazingly powerful force for good in terms of improving democracy. Yes, our role is very, very different from a newspaper publisher's.

Q167 Mr Winnick: It is open, really, to any hate merchant, until fortunately, hopefully, someone flags it up pretty quickly?
Sarah Hunter: As I said earlier, we really don't want the platform to be used for those ends—
Mr Winnick: Obviously not.
Sarah Hunter:—and we do have these strict guidelines. I think what we are talking about here is the means for making sure the platform is kept open and the means for which it is being kept clean. I think, as I said earlier, this is a rather effective way of making sure bad content is taken down as effectively and efficiently as we can.

Q168 Chair: Yes; thank you. Let us move on to the issue of criminal targeting. Mr Milner, those of us who are using Twitter declare our interest. I am a very bad Twitter user, but you have, I understand, 6 million, 6.2 million—
Simon Milner: I am Facebook, so—
Chair: Ms McSweeney is Twitter; all right.
Simon Milner: I am happy to answer any questions about Facebook.
Chair: There are 6.2 million people on Twitter at the moment in the UK, or is it more?
Sinéad McSweeney: Sir, no. Our worldwide users, 200 million—
Chair: In the UK?
Sinéad McSweeney:—and 10 million in the UK.

Q169 Chair: Facebook?
Simon Milner: In the UK, 33 million, and globally, a billion.

Q170 Chair: As far as Google is concerned, how many users do you have?
Sarah Hunter: I have to say I don't know. I apologise. I could find out for you. Obviously, we are different from these two companies, and we have about 53 different services. We have Gmail, we have YouTube, and we have Google Search.

Q171 Chair: Indeed. We have received very powerful evidence from the police and others about the way in which criminals are hacking into the internet—in particular Twitter, Facebook and other internet service providers. Ms McSweeney, is this on the increase, or is it being contained?
Sinéad McSweeney: I think that our own view would concur with some of the evidence that you have heard: that there is an increase in sophisticated, well-resourced attacks on platforms. I draw a distinction between the incident that we spoke publicly about recently, which was an attack on the platform, and the individual account compromises that people see occasionally, which generally arise from a compromise of the individual's account or their password or their email because they clicked on a link. So there are two different things.

But in terms of advanced, persistent threats from sophisticated and well-resourced individuals with expertise, with resources, there has been an increase in those, and we are currently working with law enforcement in the United States on the recent incident, but in its broadest sense it is important that there is a sharing of information between companies and law enforcement and the kind of work that you are doing here to highlight it, because it is a threat to the internet, rather than to individual companies.

Q172 Chair: Indeed. Mr Milner, do you share that concern of Ms McSweeney? Is it on the increase as far as Facebook is concerned? Are people hacking into Facebook?
Simon Milner: Yes. That is something certainly that my security colleagues would concur with: that we see consistent evidence in the UK, as you have heard from a number of senior people from law enforcement over the past several months, and in the US.

For instance, the FBI's Internet Crime Complaint Centre, which you may have come across, reports every year on the statistics on the complaints it receives about internet crime, and they have consistently reported year-on-year increases. The main areas of crime that they say are on the increase are financial scams, including criminals posing as the FBI and saying, "Your computer has been compromised. Give us your details, and we can help you out"—actually they are scamming them—and identity theft. Those are the two areas they report as on the increase, and that concurs with our own view about attacks on our own users.

Q173 Chair: There has been evidence put forward that this is coming from countries like China. Would you have a list of countries or individuals where these attacks are coming from? Obviously you have read about what is being alleged concerning the launching of attacks in China. Would you concur with that?
Simon Milner: We are certainly aware of that suggestion from the authorities, and it is very much something we leave to the authorities, to law enforcement and to international authorities to offer a view on where those attacks are coming from. It is not something that we have been public about in terms of our views on that.

Q174 Chair: For you, Ms McSweeney, I think you were referring to the recent events when 250,000 emails and other information of your users were, in effect, stolen.
Sinéad McSweeney: Yes. Our security people noted some unusual activity and quickly took action to close that down, but in the course of which they believed there was a possibility that some password information of users had been compromised, so they reset the passwords of those users and immediately notified them by email, and we also made a public statement. We don't hold a lot of personal information on our users, so it would generally be email and passwords.

Q175 Chair: Presumably, your organisations employ very clever and sophisticated people. Are they able to tell you where these attacks are coming from—which country or which individuals?
Sinéad McSweeney: In the context of the recent incident, our security people, those clever people that you talk about, are working very closely with law enforcement, and in that context, given my own

background in policing for 10 years, I would be anxious not to say anything here that might compromise or prejudice those investigations.

Q176 Chair: No, we understand that, but we have had evidence from the City of London police that most of the attacks are coming from gangs in countries like Russia and Eastern Europe, and China was also raised, but you do not have any information for this Committee on particular countries? They have it.

Sinéad McSweeney: I think they, given their expertise in the area, are best placed to make those public pronouncements.

Q177 Chris Ruane: Before you mentioned that if somebody flags up a hate crime, you will be on top of it within an hour, but what action do you take when users report that their accounts have been hijacked or that they have been victims of online scams or abuse, and how long does that process take? Also, when you are deciding to take an item down, whose standards do you use? Whose laws do you use? Is it the US, China, EU, or an amalgamation? Are there regional differences around the world?

Sarah Hunter: Shall I start on the hijacking issue? Hijacking of accounts is a significant problem. There has been some evidence that phishing emails, as in emails that have been sent to people in an attempt to try to get their passwords out of them, are increasingly coming from accounts—emails from people they think they know. Of course, they are not from people they know; they are from those accounts that have been hijacked. We spend a lot of money and a lot of time trying to prevent accounts from being hijacked in the first place. We spend hundreds of millions of pounds in keeping our users' data safe. We employ 350 security engineers dedicated to this task.

In the last two years, we have seen the number of accounts hijacked—Google accounts hijacked; that is, across all the Google products—decrease by 99.7%. We have done that by developing a technology that scans account activity and looks at suspicious activity. For example, if you have a Gmail account and you signed in from London, and then an hour later signed in from Australia, we would see that as a signal of suspicious activity, and we would ask you a few questions, some security questions; "Are you really you?" That is an amazingly effective way to stop hijacking, and as a result we have significantly reduced the number of hijacked accounts.

In the few cases where the accounts do unfortunately get hijacked, you as a user can go to the sign-in page, so the YouTube sign-in page or the Gmail sign-in page, and click, "I don't have my password. Someone has stolen my account", or whatever, and you automatically are taken through some security questions to identify that you are indeed yourself, something like, "What mobile phone number did you give us to associate with the account?" or, "What was the back-up email address you gave us when you set up the account?" Those pieces of information you would know but the criminal would not know. Once you provide us that information, we restore your settings and block the person who has hijacked the account, so it is a very, very quick and automatic service that we have put in place to prevent people being locked out of their accounts for long.

Q178 Chris Ruane: Whose standards do you—

Sarah Hunter: That is a Google set of standards.

Chris Ruane: Right, but the other aspect of abuse and slander and hate crimes, that monitoring: whose standards do you use for that?

Sarah Hunter: On YouTube, going back to the conversation earlier, our community guidelines are set by Google, and they are our own internal standards. They have evolved over the years.

We introduced a flag for terrorist activity just a couple of years ago, and that is a relatively new innovation. Those standards are things that we ourselves have set up. With YouTube, it is a platform where we own, we host all the content, we set the rules of the road, and we want it to be a platform where—is the balance right between people feeling like it is a platform they want to enjoy, they feel safe on, but also that is used for free expression? That is almost a premise of the guidelines that we have set.

Q179 Steve McCabe: I just wanted to ask you if you were familiar with a Trojan or a virus called Ukash, which I believe is spelled U-K-A-S-H, which masquerades as an official police document. I wondered if any of you had encountered that or had any complaints from your users about being victims of it.

Simon Milner: It is not something I have come across, but I am happy to ask my security colleagues, and if they have heard of it, I will write to the Committee to explain, but it is not something that I have come across from any of my colleagues involved in the security side of our platform.

Sarah Hunter: Me too, I am afraid. I can find out.

Q180 Steve McCabe: Would that be because you do not necessarily have the level of technical detail that would identify that? I am asking because I understood this was quite a common occurrence and that it is actually quite a nasty piece of work because it demands money by untraceable vouchers that are designed to permeate the system. There may be other versions of the same thing; I see you nodding. I understood it was quite common, and I was just surprised. What I wanted to ask was: what do you do about something like that?

Sinéad McSweeney: If it is of assistance, it is not something that we would be experiencing within the platform, and I think that is what my colleagues are saying. It is a common scam within email systems, rather than within a platform like Twitter or like Facebook.

My familiarity with it comes from work around crime prevention in communication in my previous job with the Irish police, where we had to highlight the fact that people may be receiving this email that purported to come from law enforcement, as my colleague from Facebook mentioned earlier, and was looking for either money or information in order to get somebody out of a perceived difficulty that the email suggested they had got themselves into. But in terms of it being within the platforms, no, that is not our experience.

Simon Milner: It is the same for us, in the sense that when people are receiving messages on Facebook, it is from people they know. We are a platform on which you have to use your real identity. You make friendships, typically with people you know in the real world, and you can only receive messages from those friends. Therefore, we do not have the same kind of email functionality, where if somebody can find your email address on a list somewhere, they can send you an email.

Something like 90% of email is spam, whereas significantly less than 5% of all the traffic on Facebook might involve some kind of spam. It is a very different order of magnitude, and I suspect Ukash—although I will ask my colleagues about this—is an email-based Trojan, rather than something that affects our platform.

Steve McCabe: Maybe I can come back later, Chairman, to the question about whether you always get Facebook messages from people you know, but we can return to that.

Q181 Chair: Yes, of course, Mr McCabe. The Norton 2012 Cybercrime Survey reported that 40% of users of social networks have said that they were the victims of e-crime, which is a very large figure. Are you surprised at that figure, Mr Milner?

Simon Milner: I am surprised at that figure, in that, as Ms Hunter was explaining earlier, we similarly use very sophisticated technology to block attempts to attack our users at the source in invisible ways that our users would never see. We are constantly updating that.

Security is an arms race and you have to be very vigilant to see what is coming around the corner and to make sure you are prepared for it, and the great majority of our users never experience a problem. That is certainly a number I don’t recognise in respect to Facebook, and I will happily look at the Norton survey to understand whether or not they break down their data into particular social media platforms, but it is certainly not something that we see on a regular basis in the UK, or anywhere else around the world, in terms of those kinds of numbers.

Q182 Chair: Ms McSweeney, what does e-crime cost your organisation? Can you put a cost on e-crime as far as Twitter is concerned?

Sinéad McSweeney: No, I couldn’t put a cost on it. From our point of view, we want users to enjoy the platform that is provided to them to discuss any range of issues, so it is in our interests to ensure that that experience is not being disrupted by e-crime. Twitter is a slightly different platform in that it is very public, so most of what people communicate on Twitter is visible to anybody who wants to look at it, so it is less attractive, even for spam activity. It is detected more easily, because it is visible if one particular account is “@-replying” lots of accounts at the same time, so from our point of view it is not—

Chair: Yes, thank you. Ms Hunter?

Sarah Hunter: We haven’t made an assessment across the board. As I said earlier, we have spent hundreds of millions of dollars to date on protecting our users’ data, so it is not cheap, but it is incredibly important. I think user trust is really at the heart of—

Q183 Chair: Hundreds of millions of dollars?

Sarah Hunter: Yes, and I think user trust is at the heart of our business model. If you think about all of our businesses, they are free, and there is lots of competition. There are lots of alternatives. If users do not believe we are keeping their data safe, they will go somewhere else, so it really is in our commercial interests to make sure the platform is kept as safe as possible.

Q184 Chair: Mr Milner, could you put a cost on it?

Simon Milner: No, it is not a number that we have ever made public, nor is it one that I am aware of.

Chair: But presumably you do spend money on it.

Simon Milner: Of course. I am sure we spend quite a lot of money on it, but it is not something where, as I said, we have released a public figure on how much we spend on that.

Q185 Mr Clappison: Perhaps I could ask Ms Hunter this question. How do private companies navigate the patchwork of different national laws when it comes to online security and data protection, and do you think there should be a more international approach?

Sarah Hunter: It is complex. The internet is a global platform and people across the world use it, and Governments across the world want to keep their users safe online. I suppose from a law enforcement perspective it is no different to international crime offline. If you are pursuing an international investigation, you have to deal with lots of different colleagues in other countries. Google Inc is a US-based company, so I think one of the key tactics or the key tools in ensuring that law enforcement can address online crime is to think of the MLAT process, the multilateral assistance treaties, and those are the agreements between the US and other countries for cross-border investigations to take place.

I looked at some of the previous evidence you had talking about MLAT and how it was a slow process, and I think that is something we should be definitely looking at to speed up. The UK and the US have a renowned close relationship, and I think if we can make that process work any better, that is surely going to help law enforcement.

Q186 Mr Clappison: Perhaps I can put the same point to Ms McSweeney, because she obviously has a different perspective on this, coming from her background.

Sinéad McSweeney: I think, again, because of the nature of the platform, an awful lot of the material that law enforcement would be interested in obtaining is available and public to them. Similar to my Google colleague, our emphasis, other than emergency requests, would be on the MLAT procedure, but that is something that we also gave evidence at the previous hearing and felt that this was something that could be improved to make it better for all of the parties to the process in terms of acquiring information.

In terms of the patchwork of laws, aside from things like law enforcement requests and data privacy, we also have country-withheld content, where if there is a tweet or an account that is illegal in one country but not in others, it can be withheld in that country. For example, an account advocating Nazi messages in Germany was withheld in Germany, and anti-Semitic content was withheld in France.

Q187 Mr Clappison: Would it be withheld here as well, then? Would it be withheld in this country because it was withheld in Germany?

Sinéad McSweeney: If the content was illegal within the jurisdiction—

Mr Clappison: It might not be technically illegal here, but we probably do not want to see it.

Sinéad McSweeney: The standards by which we judge that content are the Twitter rules and the legal content, if it is illegal—the laws of the particular country within which the report is coming from. If the content is illegal in a country, it can be withheld on request from law enforcement or Government.

Q188 Mr Clappison: Could I ask the witnesses what they think of the new European draft data protection regulation?

Simon Milner: I am happy to help you with that. It might be worth, just by way of preface, explaining that the way Facebook operates in Europe is that all users in Europe, including all 33 million account-holders in the UK, have a contract with Facebook Ireland, and therefore they are regulated under EU data protection law by the Office of the Data Protection Commissioner in Ireland. We are regulated here, and therefore of course we are very interested in changes in the EU framework that will impact on Irish national law and therefore the rules that we have to face.

We think the law does need modernising. It has been a long time since it was last updated and it certainly needs modernising for the internet age. There is a very vigorous debate going on in Brussels, as you may know, involving national Governments. We think there are some good proposals that have come out of the Commission, including the idea of a one-stop shop, so companies that are operating across Europe and are handling citizens' data should be able to be regulated in one place under a regulation that applies right across Europe, and not be subject to the oversight of regulators in each one of those countries. We think that is a very good proposal, and indeed that is effectively how we operate with the Irish Data Protection Commissioner.

There are some things that are more worrying, and—

Q189 Mr Clappison: I was going to ask you if there was anything that was more—

Simon Milner: Yes, there are some things that are more worrying, but there is a lively debate and an openness we see in the Commission and some Members of Parliament for reflecting on these. Things like requiring explicit consent every time your data is used for something new, we think that that should be content-specific, so in a service like Facebook, which people join to share their data—you do not join Facebook to keep things to yourself; you join it to share—it shouldn't be the case that every time we are introducing a new feature, you have to provide explicit consent to that.

Q190 Mr Clappison: Could you explain how exactly that would work? What is being proposed by the European Commission?

Simon Milner: Remember that there are a number of different proposals. There are the Commission's original proposals. We have had two reports from the Parliament that have contained different sets of amendments, so there are now a range of different proposals out there, but one of them is certainly requiring a much more granular form of explicit consent almost at every turn.

One of the things I hope Members will be familiar with is the e-privacy directive. How it is played out is that every time you go to a new website, you see this similar kind of banner saying, "This site uses cookies. Click here to make sure you are all right with them". If you started seeing that on more and more websites all the time, the whole experience of using those sites would become much less attractive, frankly, much more fragmented, and it would also stymie innovation. There are lots of policy-makers who agree that we have to get the balance right between allowing companies to innovate—and that is not just the likes of us on this panel, but also lots of small companies that are using our platforms and creating new data-driven businesses, including in the UK—while also allowing users of the internet to protect and control their data.

Q191 Steve McCabe: I was struck by that point about having to keep telling people about cookies. Doesn't that really mean that if you can do away with that, you are entitled to give people forced advertising whether they want to view it or not?

Simon Milner: No, not necessarily. One of the things that we should recognise is that you can offer different kinds of control. For instance, on our platform we provide very granular control that enables you, if you see an ad from a company you do not want to see, to click on that ad and tell us, "I don't want to see ads from this company again", and we will ask you why, so you can control it.

Q192 Steve McCabe: After you are forced to view it; that is my point. You are giving people something that they did not ask to see, aren't you?

Simon Milner: I am not sure that is entirely right. I think people recognise that they are getting some fantastic services for free, but those services have to be paid for, a bit like watching ITV. You expect that you are going to see adverts when you watch ITV. You don't decide what ads you are going to see; ITV does. With the kind of platform we operate, we can provide you with advertising that is much more likely to be of interest to you because we know more about you, and we can use that data to help you have a better experience.

Chair: That is enough advertising from Facebook.

Q193 Mark Reckless: Mr Milner, you said that you had 33 million Facebook users in the UK and I think around 1 billion globally. What is the number for the EU?

Simon Milner: I would have to check that and come back to you. I don't have an EU number in my head, but it will be obviously substantial. The UK I am pretty sure is our biggest market in Europe, but there are lots of other markets where we do quite well as well.

Q194 Mark Reckless: Assuming we are in the hundreds of millions potentially for the EU, isn't that rather a lot of users for the Office of the Irish Data Protection Commissioner to oversee?

Simon Milner: No, because the Facebook platform is the same wherever you are in the world. We have a single platform. There is no such thing as facebook.co.uk or facebook.ie for Ireland. It is a single platform that operates on the same basis throughout Europe, and indeed throughout the world, and therefore when it comes to the Irish Data Protection Commissioner he is able—and indeed he has over the last few years conducted a major audit of all of our data use policies and dived deep into everything we do in terms of how we handle data. He has produced a public report. I am happy to share the link to that report with you. No, in fact, he is absolutely able to handle that volume of users, because the service is the same and the way we handle people's data is the same wherever you are.

Q195 Mark Reckless: I am glad that Facebook has such confidence in him, but we were asked to have a similar measure of trust in the Icelandic authorities in respect to financial regulation. Are you able to clarify to the Committee how many staff there are in the Office of the Irish Data Protection Commissioner?

Simon Milner: I think that is really a matter for Mr Hawkes and his team, and—

Q196 Mark Reckless: You were relying on him and telling us how deep he had gone and what fantastic work he had done.

Simon Milner: I think the best thing to do would be to look at the report. They have produced two substantial reports, one in December of 2011, which runs to several pages, lots of recommendations, a highly detailed, technical report, and they brought in technical experts from outside of the Commission to help do that. They then did a follow-up report, which was published in September of last year. I am happy to share those reports, and we certainly have not had any other authority come to us and say they have not done a decent job. Certainly, Chris Graham, of the Information Commissioner's Office in the UK, recognised that as a high-quality audit of our business.

Q197 Mark Reckless: Yes. Mr Milner, you relied on the Irish Data Commissioner, and you ask the Committee to have assurance in the work that it does on the basis of that Commissioner. It is not an unreasonable question for me to ask you how many people are in the Office of the Irish Data Commissioner. I do not particularly want our Clerks to find out. I understand if you do not know immediately, but could I ask you to write to the Committee with that information?

Simon Milner: I am happy to write to the Committee, and I will also provide a copy of his reports.

Q198 Mark Reckless: Thank you. Ms McSweeney, clearly I understand the Twitter position is that the liability for all content posted through Twitter lies with the user who has posted it, but can I ask what responsibility you feel to remove hate speech or threatening content from Twitter?

Sinéad McSweeney: The fundamental basis for Twitter's existence as a platform is to facilitate the sharing of ideas and to facilitate discussion on a range of issues, and we have found that and put a premium on the fact that we don't mediate or monitor that content. However, we do take some responsibility for the content in terms of we have an objective set of standards, the Twitter rules, by which that content can be judged if it is reported to us by another user, and also, as I have mentioned earlier, the laws of the individual countries. We feel that, as a platform founded on the ideals of free speech, the only way in which we can do that is to measure content against those objective standards, because we don't want a situation where people would feel that content was not available on Twitter because of Twitter's view, as some kind of corporate view or a subjective view on an issue.

Going back to the old John Stuart Mill quote that anybody who studied jurisprudence would have studied in college, the best counter to bad speech is good speech, and in some ways the concept around community self-regulation and the process by which users and individuals are educated as to what is good speech and bad speech is better achieved when people are called out on bad speech than when it just disappears and nobody is sure of why it has disappeared. There was a recent example in recent days where an account tweeted something that many, many people considered to be offensive about a young actress who was attending the Oscars. Rather than somebody external stepping in and removing that content, the people who tweeted that themselves removed that content and apologised for it because of the outrage that they received from the community. That is not always an easy place in which to be.

It does not mean that Twitter condones the content of some of the speech that appears on our platform. However, where speech is short of being illegal—and we have seen examples with homophobic speech, where an offensive and homophobic discussion was taken over by others and ended up being a more affirming approach, so that is the approach we take.

Q199 Chair: Thank you, Ms McSweeney. In respect to what Mr Reckless has just asked you, pictures purportedly of James Bulger's killer, Jon Venables, were posted on Twitter on 14 February, and the Attorney General has said that he is taking contempt proceedings against those who posted the photographs.

I understand that this is a huge network and there is a lot of information going up on the internet, but here is an example where somebody is acting unlawfully, where the Law Officer—you have worked for the Attorney General in Ireland, I understand—has said that he is going to take the people who have posted these photographs on Twitter to court. Why are you not taking down those photographs when you know that it is unlawful for them to put them up?

Sinéad McSweeney: There are a number of aspects to this. I am conscious of the sensitivity of this particular case, and I don't want to be drawn into issues around any individual accounts. We work with law enforcement here in the UK. We have established points—

Chair: Just on the principle, as opposed to the detail.

Sinéad McSweeney: We have established points of contact with law enforcement in the UK. Where they communicate with us about content and bring content to our attention that is illegal, the appropriate steps and actions are taken by the company, and you may read into those words what you wish in the context of the—

Q200 Chair: You would expect an approach from a law officer, not necessarily on this particular case? If something is on the internet, on Twitter unlawfully, you would expect somebody to come to you and say, "We are going to launch contempt proceedings. Take it down", and it clearly has not happened?

Sinéad McSweeney: No, I didn't say that. As I say, we have ongoing contact with law enforcement in the UK, and we have established points of contact with law enforcement in the UK.

Q201 Chair: They would come to you?

Sinéad McSweeney: When they come to us, we take the appropriate action. Just to be clear, there are a number of reasons why it has to be reported to us. The first is a very practical one: it is the scale of the material. We have 400 million tweets a day, so we cannot proactively monitor and mediate that content. Also, we need to be sure. There are straightforward cases like the one you have mentioned, but there are others where we need to be clear that the report is coming to us from an authorised legal entity who is acting in good faith.

Q202 Chair: That is the only bit that concerns me about your evidence so far. I think the whole Committee accepts that the internet is a power for good. With the evidence that we have received in terms of criminality, I would just have expected more proactive activity on the part of yourselves as providers. In answer to what Mr Winnick said earlier and my previous questions and what Mr Reckless has put to you all so far, you all seem to be waiting for someone to come to you before you act. Is that unfair?

Sarah Hunter: I don't think that is fair—I think it is a little unfair, if I may. For example, we run a service called Safe Browsing. When we developed Google Search, we had to scan the trillions of web pages out there to create our search index. We have developed technology that scans those sites and that identifies where sites are hosting malware, so codes that can infect your computer. That scanning technology, this Safe Browsing technology, identifies about 10,000 websites every single day that we think are suspect.

That information we create into a list that comes up in Google Search results. You may have noticed in Google Search that sometimes there is a website, and beneath it it says, "This site may have been compromised". That tells you that there is probably malware or something bad on that site. We have developed this technology, we spent a lot of money developing this technology, and this technology is now free to other browsers to use.

We developed the list, but it is then used by Safari, by Firefox, by our competitors, to make their own search results and browsing safer. The idea that we are not taking responsibility I think is a little unfair. This is a significant investment. As I think Sinéad said earlier, we do depend on people to trust the internet for the good of our businesses, because if they don't, they are not going to use it.

Chair: Sure. We will come back to you, because other colleagues want to come in.

Q203 Bridget Phillipson: Certainly in terms of Twitter, there have been a number of prosecutions recently that have resulted from comments that people have tweeted. Do you think your users fully understand how the law works online, and how would you respond to the recent guidance offered by the Director of Public Prosecutions in this area?

Sinéad McSweeney: I think it is important that people increasingly understand that online is no different from offline, that what is illegal offline is illegal online, and in that context, when people sign up to Twitter, they agree in very simple language that they will abide by the laws of the country in which they themselves are when they are using Twitter.

There is an extent to which you can over-complicate it and talk about, "People should not have to understand the law", but an awful lot of that which becomes law is just common sense or human decency, or it is good interpersonal behaviour. The law is a way of ensuring that there is a method by which society can enforce those standards, so to that extent I think users have—as indeed across the kind of keeping safe, as well as breaking the law—their own obligations to educate themselves about how to stay safe, how to stay secure online, but equally they need to deploy their own judgment about how they use the platforms in the context of the laws of the country in which they are.

Simon Milner: Perhaps I can help on the Director of Public Prosecutions point. That is an area where the law is different online than it is offline, in that you can say some things in this space, in a spoken way—and indeed I have heard Keir Starmer talking about this. He could say things in a public forum that would be perfectly legal. If he put them in an email or in a Facebook message or a tweet, they would be illegal, and it is one of the ways in which the online and offline are not properly aligned, and something hopefully the Government will look at as it looks at the Communications Act in the coming years.

Therefore, the approach that Mr Starmer is proposing, and indeed he is already asking public prosecutors to adopt, we think is the right one. He has it spot on, but he should focus on the context and the harm that might result from a communication that might, as it were, accentuate the impact of it, rather than just exactly what was said in the communication itself. We are very impressed by the analysis, and we think he has it spot on. I guess the proof will be in the pudding as it plays out over the next several months.

Q204 Bridget Phillipson: Just one follow-up to Ms McSweeney. There was a case just last year where a rape victim was named repeatedly via Twitter. Clearly, the responsibility for doing that is the responsibility of those who choose to post that content, but is that something that you have learned from? How would you respond to that then and now? Is there any difference?
Sinéad McSweeney: Again, we would have to be aware that it was happening, because we won't necessarily know that it is happening on the platform. Again, where issues like that are brought to our attention, we can take action. The naming of rape victims—again it should be obvious to most people that that is not something—you do not have to know that it is illegal or that it is contempt, because in some senses in personal, offline conversations we tend to talk about rape or the victim of rape in whispered tones. We know that it is a sensitive issue, so why people would change their behaviour when they are online is different, but again, the issue—if it is flagged, if it is reported to us, yes, we can take action.

Q205 Bridget Phillipson: It is just the number of people that you can reach with such a message is far greater than a conversation you might have with one or two people. You could potentially reach millions of people, as opposed to a conversation one-to-one or in a small group. That is the damage, isn't it?
Sinéad McSweeney: Yes, it is. It is, potentially, and that is why, for example, the Law Commission here is currently doing a substantial consultation on contempt, and we have attended the symposium and are taking an interest in that, because the world has become more complicated.
Chair: Thank you. I should say to colleagues and witnesses that we are expecting a vote shortly.

Q206 Mr Winnick: Ms McSweeney, arising from the replies you gave to Mr Reckless and to the Chair, I am slightly concerned because, without putting words into your mouth, I think you said, in effect, rather like Ms Hunter previously, that there is a debate and that people can put their views—obviously they can—and then if there are complaints, the matter will be looked into. You see, if someone on Twitter said, "Hitler was right", or, "The Holocaust never occurred" which is not a criminal offence in this country—there is no reason why it should be—or a rape victim very much in the media "asked for it"—such a crude sort of description, and absolutely disgusting—presumably that is simply on Twitter and, until someone complains, it remains on Twitter. Am I right?
Sinéad McSweeney: But those events, those instances that you talk about, don't just happen on Twitter. People stand up in football stadiums and hurl racial abuse at players on the field. Those—

Q207 Mr Winnick: Does that justify going on Twitter?
Sinéad McSweeney: Those around them will call them out on that, and similarly on Twitter, rather than Twitter deciding as a corporation or as a bunch of individuals whether that is good or bad. Our approach is that the other users of the platform decide what is good speech and what is bad speech. Also, we do give users the ability to control their own experience. If I have a particular set of interests, that is what I will get from Twitter. I may never see a tweet about football or golf or sport in general. I will see lots of tweets about politics, about policing, about things in which I am interested, so people can define their own experience. The problem is that taking the bad speech away doesn't remove the thoughts from somebody's mind, doesn't remove those sentiments from society, and sometimes is it better to see those thoughts and see them challenged than to just remove them from the public mind and public view.

Q208 Mr Winnick: So, anything should really go on Twitter until someone complains?
Sinéad McSweeney: No, we don't say that anything should go on Twitter. We have a set of rules, we have rules by which we believe our users should behave, and we also ask that our users obey the laws of the countries in which they live.

Q209 Mr Winnick: The examples I gave of someone, sick in mind, obviously—"Hitler was right. The Holocaust never occurred", or, "The rape victim asked for it"; that could and would go on Twitter?
Sinéad McSweeney: There are individuals who stand in universities and make those statements.

Q210 Steve McCabe: It does sound as if you are coming dangerously close to describing yourself as the innocent arch-facilitator, that Twitter trolls are the responsibility of everybody else and that cyber-bullying is entirely the responsibility of those who do it. I do not deny their responsibility, but it does seem to me they are able to do it with enormous reach because of the service you provide, and if that results in a youngster deciding to take his own life or some other tragedy—certainly the parents of a child who killed themselves in my constituency have met with Facebook staff—surely if it results in that, you have to go back and examine what you do and decide what more you can do to control this thing that you have unleashed.
Sinéad McSweeney: I do not think we are standing back from our responsibility. I know that within Twitter we have—

Q211 Steve McCabe: What is it that you have done that you have not told us about so far that shows you taking more control and responsibility for it? Because what I have heard so far is how you react when somebody else takes control and reports it to you.
Sinéad McSweeney: I think there are two sides to that. On the safety side, not only do we have a set

of rules by which users' behaviour is measured and observes the laws of the country, we also have a hugely—densely, almost—populated safety centre with advice. There are safety tips for parents, teens, teachers—like all of the other companies here, we participate in Safer Internet Day. We have relationships with all of the key organisations in this space, and just as the bad speech, as you would term it, reaches millions of people, those safety messages, that advice, those resources that are there to help people who are experiencing bullying, who are experiencing depression or mental health difficulties are also there on all our platforms and accessed by the individuals who are vulnerable and who are helped by them.

On the security side, again, yes, we talked about the instances that are flagged to us, but, as I know only too well from 10 years in policing, the best antidote to crime is prevention. It is all very well to react to a crime, to detect a crime, but the best activity that any law enforcement involves itself in, or corporations like ourselves, is to educate people.

Q212 Steve McCabe: But I am asking you how you are preventing. I hear a lot about how you react when something has happened and somebody reports it, and you say you have some warning material displays, but how do you prevent it? It happens persistently.

Sarah Hunter: Shall I give an example of something we have done at Google, because obviously we have been around a bit longer than Twitter? There was a case a couple of years ago where there were some suicide cases, and they were, in the inquest, reported to have used Google Search to identify ways to harm themselves and eventually, sadly, kill themselves. There was quite a public outcry about this and, sort of, "What can be done?"

We met with the Samaritans to talk about this, because obviously no one wants to see these sort of cases, and we are companies run by human beings who feel responsible, so we wanted to talk to them about how to prevent this sort of thing from happening. Some people were saying, "You should just remove all sites that mention how to kill yourself from the internet. You should just block them from the search". The Samaritans said, "No, that is not how we think you should react, because a lot of these sites are sites where people go and talk and find people with common interests to help them not kill themselves. They are support groups as much as they are information sites". Their preferred response, and what we ended up doing, was when someone searches for "How to kill yourself" on Google—

Q213 Chair: Sorry, could you just clarify? You are telling us that a website that says, "How to kill yourself" is actually a support group to help to keep people alive?

Sarah Hunter: In some cases, the sites they were referring to were actually self-help forums for people who are feeling depressed, and someone saying, "I want to kill myself"—"Well, no, don't kill yourself", and they were as much forums for preventing suicide as they were for—but the Samaritans' solution, and this is going back to the original question, was that when someone searches for "suicide", an advert should come to the top of the Google Search box, saying, "Are you feeling depressed? Do you want to talk to someone? Call the Samaritans". So the searcher was prompted to go and seek help, rather than going to one of the more invidious sites, so I think there are ways—

Q214 Chair: So, you do that now?

Sarah Hunter: We do that now, yes.

Q215 Chair: Would you do that for other areas, for example, somebody who was following the site of Anwar al-Aulaqi? Would you have a little thing going up saying, "If you want to blow people up, come to this site instead"?

Sarah Hunter: We do offer a service for all charities; that they can get free advertising, up to $10,000 a month worth of advertising on Google, so a lot of charities do take up that offer. I can't think of another example. Someone like the NSPCC is—

Q216 Chair: Would you give us some of those examples? It would be very helpful if we had examples, if you could write to us—

Sarah Hunter: Absolutely.

Chair:—of where you have now put up a banner when people search against a particular site, and there—

Sarah Hunter: It is the charities who do that, not us, but yes—

Chair: No, but if you could give us examples—because you must have it, because obviously you do not give it away free.

Sarah Hunter: We do. It is free for any charity.

Chair: All right, so you would have a list of all these? If I could have it—

Sarah Hunter: Yes, I do. I will happily do that.

Q217 Steve McCabe: Chairman, if we are going to get those examples, could we get a little bit of background on how the charity was selected? The example you quote is very—

Sarah Hunter: Any charity can do it.

Steve McCabe: Yes, but what I am saying is the example you quoted where the Samaritans came to you, that is rather obvious. I would interested to know how other charities have been—

Sarah Hunter: I am happy to do that.

Chair: Along with the statistics of how many complaints were made and how many sites were taken down?

Sarah Hunter: Of course.

Q218 Chris Ruane: This is to Simon Milner. We understand that some models of HTC mobile phones have a Facebook app in the root directory which cannot be removed or reliably turned off, which therefore transmits information about the owner's internet use back to Facebook. Are you aware of this, and do you think this respects users' privacy and their right to choose whether or not they wish to share their data with Facebook?

Simon Milner: That is clearly a highly specific question and one that warrants a highly specific answer that I do not have, but I am happy to write to you afterwards. I will investigate it and come back to you.

Q219 Chris Ruane: This one is to Sarah Hunter. Google has previously been criticised by 10 Information Commissioners for not taking adequate account of users' privacy. It has since been fined $22.5 million by the Federal Trade Commission for side-stepping security settings on the Safari web browser so that it could track users' internet use. What impression do you think this gives of Google's respect for users' privacy?

Sarah Hunter: We deeply regret both of those incidents. As we said separately at the time, they were mistakes. We did not intend for that to happen, and as soon as we identified it, we owned up, we were very public about it and we tried to rectify the coding mistakes and make amends. Users trusting us and keeping their data safe is incredibly important for us. We take it incredibly seriously, and I think it is our responsibility to try to earn that trust back when things like that happen.

Q220 Chris Ruane: How have you done that? How have you earned that trust back—or have you?

Sarah Hunter: In the UK, the ICO did investigate us; and they annually audit us now, and we have made a number of changes to our processes internally as a result of that audit. In fact, they are due to come back again very soon, so it is an ongoing process. We always want to improve, but the ICO audit is part of that process.

Chair: Thank you. I am afraid we are going to have to stop; not quite saved by the bell, because you have been here for an hour and a quarter, and we really are very grateful to you for giving evidence. It has been most enlightening.

Sarah Hunter: Thank you for having us.

Chair: We will write to you with further questions. There are a number of issues that we wanted to take up with you before we complete our inquiry, but we are very grateful. Thank you.

Tuesday 16 April 2013

Members present:

Keith Vaz (Chair)

Mr James Clappison
Michael Ellis
Dr Julian Huppert
Steve McCabe
Mark Reckless
Chris Ruane
Mr David Winnick

Examination of Witnesses

Witnesses: **David Livingstone**, Associate Fellow, International Security Research Directorate, Chatham House, **Professor Sadie Creese**, Professor of Cyber Security at the University of Oxford and Director of Oxford University's Cyber Security Centre, and **Dr Ian Brown**, Associate Director of Oxford University's Cyber Security Centre and Senior Research Fellow at the Oxford Internet Institute, gave evidence.

Q221 Chair: I call the Committee to order and ask our witnesses to excuse us if there is a Division in the middle of your evidence session. We think that is likely because there are a number of pieces of legislation going through today. What will happen is that I will adjourn the Committee for a certain period of time. However, we will come back, so don't feel that you are being abandoned.

Can I welcome everyone here to the Committee's continuing inquiry into e-crime, and could I ask Members to state if they have any interests that go beyond the Register of Members' Interests? I will start with a question to all our three witnesses concerning the statement made to this Committee by the head of the City of London Police, Adrian Leppard, on 11 December. He told the Committee that he felt that the war against internet crime was being lost. Mr Livingstone, do you agree with that?

David Livingstone: The first point is about defining "the war" in that context. This is obviously going to be an ongoing issue the more that the internet becomes integral to our lives. Whether it is being lost—and therefore what is the definition of a victory or a loss—I would call into question. There are certainly issues with the amount of crime that is being committed, and whether it is increasing proportionately or whether we are now on a track where we can start taking positive steps—

Q222 Chair: You pose a lot of questions back at the Committee, but you are not giving us any answers. What do you think? Do you think that it is being lost?

David Livingstone: It is serious. It is getting worse, but I think with the strategies that this Government are putting in place, there is a possibility of closing that gap, especially if we can work with pace and agility to match how the bad guys operate inside the internet.

Q223 Chair: Thank you. Professor Creese?

Professor Creese: With the issues of definition aside, I suspect it is not currently being lost. If it were currently being lost then we would see people withdrawing from cyberspace in many areas, and we are not. However, we are continuing to witness losses and we are continuing to witness concerns. Personally, I think that the losses and the level of threat are going to increase dramatically, as we continue to expand our dependency on cyberspace, and that we are in this operational environment where we will continue to have to fight that war on an ongoing sense. So there will be times when we are ahead and times when we are behind. We are never going to win it.

Q224 Chair: Dr Brown?

Dr Brown: I would agree with my two colleagues' comments and say that all crime is a continuing arms race between the perpetrators and the defenders. Trying to win this war needs a broad spectrum response from a number of areas of government. I think the UK Government are on the right lines in developing law enforcement, so the UK is going in the right direction. Persuading other countries to take some of the same kind of actions will be important, as the UK Government are trying to do.

Q225 Chair: The other point that he made to us—in very powerful evidence to this Committee—was that Britain was being targeted by gangs, specifically from countries such as Russia and eastern Europe, in the cyber-wars. Do you agree with that?

David Livingstone: That probably reflects the fact that we have quite a mature digital economy and the fact that we use the internet for many things. The amount of valuable and attractive goods and items that can be found on UK-based IT systems is probably a relatively rich hunting ground for organised criminal gangs, so they are attracted here.

Chair: I am going to stop you there because the bells indicate a vote. I am going to adjourn the Committee until we are quorate, which I hope will be at three o'clock. Thank you.

Sitting suspended for Divisions in the House.

Q226 Chair: We are quorate, so we will resume our proceedings.

Mr Livingstone, I had asked you about the evidence given by Adrian Leppard, namely that gangs have been targeting the United Kingdom, especially from Russia and eastern Europe. Is there evidence of that, Dr Brown?

Dr Brown: I think we have seen quite a bit of evidence that organised criminal gangs have moved into cybercrime and are specialising in the different aspects, whether that is writing the software that will target systems, transferring the money or paying the money mules to take the cash out of the system. I agree with my colleague's comment that, of course, the UK is targeted because it is a rich country where there are a lot of resources worth targeting. I would not go so far as to say we have crystal clear evidence that the UK is top of the list, but I think in general, yes, it is a target.

Q227 Chair: Professor Creese, what is a better way of ensuring co-operation between different countries in dealing with internet crime? One of the aspects of this whole issue that interests the Committee is that countries seem to be doing things on their own and not necessarily seeking to share information. Are organisations such as Europol and Interpol an effective vehicle to bring together the good guys in dealing with those who are seeking to break into systems?

Professor Creese: They are a vehicle—one of many. In fact, there are already numerous initiatives on the international stage seeking to increase knowledge, so the UN, UNESCO and ITU. There are lots of international organisations working in this space. Also, if you look at some of the single organisations and bodies, they are working more closely together within their own communities. One of the key issues, as we see the levels of cybercrime rising—which they will inevitably even as they ebb and fall—is how we scale up our response. You will have seen in the various written evidence submissions that you have received that we are certainly making a huge investment in the UK to do that, but in truth we are probably going to have to invest more over the next 10 to 20 years.

Q228 Chair: Because it is the framework, isn't it? I visited Interpol last week. It recognises the fact that we are in a new game dealing with the power of the internet, but it seemed that countries were not willing to share that information.

Professor Creese: It will be variable from country to country. The challenge that we have is that the special relationships you can establish between any two countries will be unique and will require their own processes. What we need to do is to generalise these processes, standardise them and speed them, so that when we need to seek evidence in the face of crime we can do so at speed. The challenge we have at the moment is we are limited in our ability to do that.

Q229 Dr Huppert: It is good to see you all and, Professor Creese, we had some interesting discussions in another context before. I would like to ask about some of the issues involving consumer use of technology, so the prevalence now of social media, Facebook, Twitter and so forth—I am guilty in that respect myself—but also the widespread use of Google and things like that. People are sharing far more information. How effective do you think these various tech bodies are at trying to manage both the safety of the information and privacy, which is a related issue? I am happy for any of you to start.

Dr Brown: The two companies you have mentioned have absolutely invested a lot in protecting their own infrastructure, especially—

Q230 Dr Huppert: I think I mentioned more than two. Which two were you referring to?

Dr Brown: Sorry, I was thinking of Google and Facebook in particular. They certainly have invested a lot in protecting their own infrastructure. Clearly they are targets themselves. We have seen that especially with Google. Some of the initiatives it has taken with things like two-fact authentication, where Google will now increasingly send a passcode to your mobile phone, for example, if you log on from somewhere new, are exactly the kind of things we need. On the privacy side, as the Home Office said in evidence to you, looking at things like privacy by design, which the European Commission has proposed in the European framework, is very important. If we are going to see systems that will potentially have gigantic amounts of information about individuals, make sure that only relevant and pertinent information is collected in the first place, and is kept only for the amount of time it is needed, rather than just taking the approach of throwing everything into the pot. No matter how good your information security is, even companies like Google—real-world experts in doing it—are not going to be able to defend against every attack, as we saw with allegations of Chinese hackers breaking into its system.

Q231 Dr Huppert: You are focusing on the defences against attack but, as I understand it, with Google+ the account settings are set to "public". Facebook allows a whole range of third-party apps with very little safeguard. People may not be able to attack through some routes, but it seems to me there is a whole series of holes there that do allow a lot of information that could perhaps be used for other purposes to make attacks on other systems easier.

Dr Brown: I think those default settings are absolutely critical. That is the other part of what the European Commission is doing—talking about privacy by design and by default—so that the settings are protective and if people choose to open up, that is fine as long as they are aware of the consequences.

Q232 Dr Huppert: Very quickly, just to finish on that. If all that the European Commission is doing in this space and these areas happened, would that solve the problem?

Dr Brown: I think it will take us a long way. I don't think it will solve it.

Professor Creese: Thank you for the brilliant comments. I will address another issue—the related issue that you were just getting on to—which is: if people choose to put it out there, that is their business. One of the challenges that we face is that, in general, people do not have a good understanding of the risk. There is something very unique about cyberspace and the data you put into it, in that it is persistent: it does not get forgotten; it can be mined. Often people find years later that they have forgotten about data they have put out there. Yet in the meantime, people are able to aggregate and mine that data, and very often learn stuff about you and the choices you are likely to make, which you are probably not even conscious of yourself. That is perhaps the issue. Focusing on the privacy risks associated with big data, social networking and the like is the question of how we enable people to make good and safe decisions so that, in effect, they are managing the risks.

Some of the research we have been involved in has been looking very specifically at the bleed between domestic lives and work lives. If people are engaged in these kinds of technologies in their domestic lives, could that be used to introduce vulnerability into the enterprise through more enhanced targeting? In truth, probably, yes, we are in a situation where that could be the case.

Chair: We will explore that further with Mr Winnick when he comes to ask his questions.

David Livingstone: I think there are a couple of other questions here. Where does the data end up? Under what legislative arrangements is that retained? For example, much of the data that users in the UK put on Facebook may end up in California, where privacy laws are quite liberal. The data accumulated by Facebook on many individuals from a lot of countries may be shared quite freely—more freely than it would be if it was UK-based data. The other thing is that there are 1 billion users now on Facebook. This is a very, very big organisation with a lot of data held. I am not sure if we know the figures about how many times it has been hacked successfully—perhaps they do not even know themselves—and I do not think we know too much about how its security arrangements work, so there is that risk that more data are leaking away than one would want. That is not just Facebook; that is any large social networking organisation.

I agree with Ian and Sadie here that people are putting data on there that in the long term they might regret. As part of Chatham House's research in the last paper we were writing with directors of a major UK high street bank, the comment was, "People are giving away information on social networks quite freely, and giving away information that we want them to keep private," such as dates of birth and all those kinds of things that are there to establish identity for financial safety.

Q233 Dr Huppert: That is exactly what I was getting on to, because Andy Smith from the Cabinet Office recently advised at a publishers' internet conference, just around the corner from here, that people should use fake names and fake dates of birth wherever possible. This caused a bit of a storm, but is it something that you would all endorse? I see nods—just for the record, which does not always capture nods very well. Professor Creese?

Professor Creese: Yes, although in truth some of that data are obtainable through other routes. Not putting it on Facebook does not necessarily remove it from the hands of those you would prefer to remove it from. If I may just extend this debate into something that we all—

Chair: Can I just say not too wide, because we have a lot of questions.

Professor Creese: Not too far, but it is important not to see this just through the lens of social networking. You will all be carrying smartphones, no doubt, and you will all be downloading apps from unknown creators, and the location-based services and functions that almost all of us engage with day to day—and will increasingly do so—are enabling a whole range of data to be collected and shared. That is not managed in the same way as you might do in a social networking environment, and that too poses an element of risk. One of the things I would like to see happen is a much more enriched understanding of how we manage consents around the sharing of personal data, and to encourage people to see that as a lifecycle and not a one-off blanket "I accept these terms and conditions", when five years later I have forgotten what I accepted. That is very important to maturing our society in this space as we move forward in the 21st century.

Q234 Mr Winnick: I am afraid that modern technology has had no effect on our going up and down the stairs and voting, but that is part of parliamentary life I think.

Can I follow up, Professor Creese, and your two colleagues? To a large extent, you have dealt with or touched on the question of public awareness. I don't know if would you share it, but I get the feeling that ordinary members of the public—including ourselves around the table, for that matter—do not realise, to the extent that they should, the dangers involved in e-crime and the illegal practices of gangsters in the various gangs. Do you feel the Government or some public authority, or a new public authority for that matter, could do more? Who wishes to answer—as the Chair would say, briefly?

Dr Brown: I think the Get Safe Online programme that the UK runs is a good example of how you can get information out to people, but I don't think it goes far enough. As you say, it is not something that the broader population is as aware of as it should be. To some extent that needs some social learning. Unfortunately, it takes people to know someone who has suffered a loss really to understand the potential, in-depth. Just reading about it or seeing it on TV is not perhaps getting through to people quite strongly enough yet.

Q235 Mr Winnick: You have answered the question. May I ask another question that your two colleagues could answer? What about an advertising campaign? The advertising people claim that they do all kinds of wonders. Perhaps I have missed it, but I have not seen any sort of advertising campaign warning people about what could likely happen. Do you think any purpose would be served, Mr Livingstone?

David Livingstone: I think there are many routes that you could take to make the public more aware of the vulnerabilities of cyberspace and how to use it with less risk. There are a few points I would like to make. One is the amount of money being spent at the moment by central Government on cyber-security public awareness. The NAO's recent report put that at £4 million out of the £260 million that has been spent so far out of the national—

Q236 Mr Winnick: But £4 million is a drop in the ocean, isn't it?

David Livingstone: That £4 million represents 2% compared with some other figures that were quoted in that report. So, for the high-end threats, it is £157 million. We have a dissonance here with the director of GCHQ saying that 80% of the problems could be fixed just by getting the basics right. However, generally it may be said that the population do not know what those basics might be, for example automatic patching, making proper use of anti-virus and knowing where the risky parts are on the internet. Perhaps there is a little bit of an imbalance there about the resources being deployed to create better public awareness. Although, then, it is not an easy issue. You have all sorts of segments of society: you have old and young; you have business and private; and you have communities and so on.

Then there is the method—not only the messages, but how you get the messages across. There are some interesting things that one could take from best practice in other areas, such as the messaging from the Department of Health on health matters that is focused on individual groups to send out very different messages—perhaps sexual health for 16 to 25-year-olds.

Q237 Mr Winnick: What about smoking?

David Livingstone: Also for flu jabs, to focus more on the elderly population. The modes of delivery and what you say on all those are vastly different, and perhaps some of those mechanics of communication can be taken forward into the cyber world.

At the moment, I am helping the Scottish Government with their cyber-security statute, which is in the context of the devolved Administration. We are putting the public communications responsibility for developing that strategy as not a Government thing, but a business, commerce and law enforcement thing, where they are developing the means of communicating about cyber-security risk rather than the central Government. They are almost appealing on behalf of the people that they are—

Q238 Mr Winnick: You are doing this at the moment with the Scottish Government?

David Livingstone: Yes, we are.

Q239 Mr Winnick: How long have you been doing this?

David Livingstone: About a year.

Q240 Mr Winnick: Thank you. Any comments, Professor Creese?

Professor Creese: You have had lots of excellent input. I completely concur that different demographics require different messaging, some of them primetime telly and some of them viral YouTube videos or music videos, no doubt. A point worth making is that Get Safe Online and other Government initiatives have been fantastic, and I would imagine that, historically, what we have done is under-resourced in the communication element. We have the expertise; we understand the messages that we need to transmit. The 10 steps for board members that was launched last September is another good example. I know that 10 steps for SMEs is being looked at. Yes, I agree that we need to invest in getting the message out there and that it will require diversity in delivery, and I believe that is already on the agenda.

Q241 Mr Winnick: I like what your colleague has just said about the way in which the Health Department has spotlighted, be it on sexual health, smoking or indeed excessive drinking.

Professor Creese: Public health campaigns are an excellent example. You can have a look at some of the successes that they have had, using fun but scientific programming around public health and body awareness among the younger population. *Embarrassing Bodies* was one series, and there was a hugely successful campaign on the internet alongside that programming. There are experts out there and I know these kinds of things are already on the agenda, certainly with the e-Crime Reduction Partnership that the Government set up. I feel positive that people are embracing this.

Mr Winnick: I am sure the Committee will take that very much into account. Thank you.

Q242 Steve McCabe: I think the Government have arrived at a statistic that says that cybercrime is costing the UK £27 billion per year. I notice you laugh. How accurate do you think that figure is, and do you have any suggestions on how we could get an accurate measure on this?

Professor Creese: I have not seen the working out that arrived at the £27 billion number, so I can't critique it from a scientific viewpoint. The fact that we have not seen good evidence behind it would say that perhaps we can't give too much weight to it as a particular number.

Dr Brown: I have a very good paper here that critiques it—I am sure you have seen it—that Ross Anderson and colleagues wrote. I think, as he says, that there is not good evidence for the £20 billion component of that £27 billion that Detica had attributed to business costs. Ross and colleagues produced much more detailed evidence. Some of it is on the much smaller side, so hundreds of millions of dollars, looking at things particularly like patent-infringing pharmaceuticals, for which they estimated $40 million in loss. Some is potentially very significant in the longer term, like the welfare and tax fraud that they thought could cost many billions as those systems move online, as the Government are doing to save costs. As Sadie said, showing the working out and having peer-reviewed scientific papers that can be looked at year after year, which Parliament can look at and which other scientific experts can comment on, and keeping those figures up to date, is the way to do that.

David Livingstone: Trying to put a figure on it holds you hostage to fortune, but I think we can easily say that the losses are very large. Of course there may be losses that we do not know about because we have not yet detected the intrusion into servers that, for example, might hold critical and very valuable intellectual property. However, it is interesting to note that it has been a long time since the Government have actually mentioned £27 billion as this figure. Indeed, I note that when Mr Maude was launching the Cyber Security Information Sharing Partnership just a short while ago, he quoted "numbers of billions". So I think he has veered away from trying to put a precise figure on the scale of loss or harm to a more generic figure, which I think is probably appropriate.

Q243 Steve McCabe: Dr Brown, if I could ask you something in particular. I think this report you have been working on with the UN said that two thirds of the states involved did not think their own crime reporting systems were adequate to deal with this problem. Do you have any suggestions about how people could develop more adequate crime reporting systems?

Dr Brown: The least controversial recommendation that the UN made in the report you are referring to was that there are many countries—not just in the developing world—that need a lot of help on capacity building, with advice from states that have more experience in Europe and North America. Obviously, there is a wealth of expertise in industry and academia to help them to do that. The recommendations that became more geopolitically controversial were how far states should be treaty making and taking things like the Budapest convention, and trying to broaden that out to cover some of these states so that they weren't just improving the evidence, but updating their legal framework and making it possible to co-operate with law enforcement agencies from the UK and elsewhere in dealing with these crimes.

Q244 Chris Ruane: Turning to the role of the police in combatting digital crime, given that digital evidence is now a factor in so many crimes, what strategy do you think the police need to adopt to increase their capacity to process it? Do you think there would be any merit in outsourcing digital forensics?

Professor Creese: We have seen written evidence to this Committee on strategies that have already been taken, which from a personal stance I think are very good. In terms of the outsourcing of the gathering of forensics, I think one needs to understand that in the context of how you would maintain quality. There are always costs associated with how you regulate the sectors that are going to be working on your behalf, and what kind of standards you will require them to comply with in terms of their behaviours, how they train their staff and the processes they engage in, so that you can be sure that this evidence maintains an adequate standard. Of course we are lucky enough in the UK that we understand these things very well, but I would encourage you to look very hard at those kinds of costs in the round. We obviously need to scale up. I can see why we might well consider outsourcing simply to reach the scale, but we would need to think very hard about how one ensured that we maintained quality in the face of that.

David Livingstone: There is an issue here about calling on capabilities that already exist—for example within the financial services industry, where they do a lot of network analysis of where the current attacks are coming from—to establish almost the public and private partnership relationship with law enforcement laying down criteria, which would then make useful evidence. The thing that I think is most important is how quickly this information, intelligence or evidence can be made available to law enforcement as well, without the necessary use of production orders and so on, which can take quite a long time before evidence can be made available for a criminal pursuit. Forensic analysis is very expensive indeed, and one has to be very careful before you commit to doing it in house. There is a compelling case that some element of the forensic pursuit of criminals needs to be performed outside the law enforcement estate. How those relationships are actually developed I think we will have to see over time. The speed at which this information can be made available, without going through cumbersome processes of production orders and so on, I think is a key point here.

Q245 Chris Ruane: How do you rate the current digital forensic capabilities across the UK police forces?

David Livingstone: I would probably say that they are starved of resource. They are very good, but they can't cope with the volume of crime that is occurring.

Professor Creese: That is going to be true for any type of crime, not just cybercrime. From my personal experience, I have always been very impressed by the professionalism, but clearly they could always benefit from more resource.

Just to reflect on your question on outsourcing, I wonder if in part that might ease the international dimension of gathering of evidence. At the moment it is very challenging to gather evidence across national boundaries, but if we were outsourcing internationally, that might help to overcome some of the latency in that system.

Dr Brown: At the same time, some of the reasons why production orders can take some time is that you have to make sure that you are being proportionate in the information you are asking for. We don't want to wave a wand and say, "We will just hand over all this data and completely trust the law enforcement intelligence agencies," in a way that we have not in traditional justice systems.

Chair: Thank you very much. This is fascinating stuff. We may well write to you with further information and to ask for further facts about this area. We are most grateful. Apologies again for having to interrupt your evidence for the votes, but I am afraid democracy has to march on even for the Home Affairs Committee.

Mr Winnick: They helped to educate us about this.

Chair: Indeed. Thank you very much. We are most grateful.

Examination of Witnesses

Witnesses: **Anthony Browne**, Chief Executive, British Bankers' Association, **Matthew Allen**, Director, Financial Crime, British Bankers' Association, and **Katy Worobec**, Head of Fraud, Financial Fraud Action UK, gave evidence.

Q246 Chair: Mr Browne, Ms Worobec and Mr Allen, thank you for coming. We are coming to the end of our inquiry into e-crime and we are most grateful to you for coming here. Apologies for keeping you waiting beyond the time listed on the Order Paper.

Can I start with you, Mr Browne? What kind of figure do you put on the cost to the banking sector of online fraud every year?

Anthony Browne: It is actually the FFA UK that is responsible for collecting the figures, but in 2012 they are £475.3 million for online banking, plastic cards, cheque and telephone banking fraud, which was in fact less than 1% of total fraud in the UK. That is against a sector that is about 8% of GDP. So it is about 8% of GDP and 1% of fraud. Specifically online banking fraud—against people's online accounts and so on—was £39 million, which is down about 25%.

Q247 Chair: It sounds like a large amount that is being taken from people's accounts.

Anthony Browne: It is. One pound of fraud is—

Q248 Chair: You said it is going down. Is it on the increase in fact overall?

Anthony Browne: Again, it is quoting from FFA UK figures.

Chair: This is not individual. It is not *The X Factor*, so feel free to chip in whenever you want to.

Anthony Browne: It is still at a high level. The general story is going down over the last 10 years, although it has tipped up a bit in the last year. You say it is a lot of money. Clearly it is, although as a whole the banking sector has a good story to tell, given the size of the sector and 26 million online accounts. That is a result of the amazing amount of work that the industry puts into this. It does take it very, very seriously. It puts huge amounts of resources and technology into combatting it and the FSA is the front line of that co-ordinating industry response.

Q249 Chair: In terms of those figures, are there any other figures that you think the Committee might be interested in, Ms Worobec?

Katy Worobec: Yes. To drill down a little bit to the online fraud, in the figures that we collect, there are two aspects I think you will be particularly interested in. One is online banking itself, which is the figure that Anthony mentioned of £39.6 million in 2012. The other aspect is online card fraud, which cost the industry £140.2 million in 2012. If I look back, we saw peaks in both those types of fraud. The peak for e-commerce fraud on cards reached just over £181 million in 2008, so we have seen it drop around 23% since then. At the same time, we have seen online card spending increase from £41 billion in 2008 to £68 billion in 2012.

Q250 Chair: So what does that tell us?

Katy Worobec: I think it says that we have been reasonably successful in reducing online fraud in that space, at the same time as spending in that channel has been increasing rapidly. In a similar vein, if I look at the online banking figures, the peak of the losses that we have been recording saw it reach just over £59 million in 2009. As we said, it dropped to £39.6 million last year. At the same time, users of online banking have increased from 22.4 million in 2009 to 26.8 million in 2011, which are the most recent figures that we have in that space. Again, users have gone up 20% while we have been able to see the fraud dropping over that period.

Q251 Chair: Mr Allen, is this done by organised groups? Are there people in a room somewhere in Europe, or even in the United Kingdom, who are saying, "We are going to use our skills? We are going to pool our skills in order to break into people's bank accounts and steal money"? Is this organised, or is it just—

Matthew Allen: Yes. Feedback from our members, as well as evidence from Europol and other international bodies, demonstrates there is an international element to cyber-offending and that there is a degree of organisation within the crime networks that operate in this area. I think it is important not to generalise. There are different aspects of cyber-offending that will be perpetrated by different groups and in different ways. Generally speaking, our assessment and that of international bodies is that there is an international and organised element to this.

Q252 Chair: Would you have a league table of the countries where this is coming from or groups of people, or is this just impossible to pinpoint in the way that I suggest?

Matthew Allen: No, we don't have a league table within the British Bankers' Association. We have contributed to a number of Government exercises to provide our expertise of the nature of some of these threats. I would also add that the international nature of the threat is not solely a cyber element—fraud, money laundering, and other types of financial crime often have an international element as well.

Q253 Chair: Do you think we ever get to find out who is responsible, or is it just a case of satisfying the customer? I give the example of my PayPal account that was hacked into. Attempts to get to PayPal to find out whether it had caught the people responsible were impossible. Once you had pressed all the numbers and listened to all the music and got to customer service, nobody would ever tell you who was responsible. It satisfied me because it put the money back into my account, but is there a feeling that people are just satisfied in that way and there is no attempt to get to the bottom of who is responsible?

Matthew Allen: In the United Kingdom, the National Fraud Intelligence Bureau has been established and housed within the City of London Police. That provides a central body to bring together intelligence from a range of sectors.

Q254 Chair: Yes, but give us your intelligence. You must know about these things. For example, how many people were prosecuted last year?
Matthew Allen: I don't have the figures to hand.

Q255 Chair: Does the prosecution system work? Are you pleased with it? Do you think they get to the end of the tunnel, or is it just a case of people getting the money back into their account, so everyone is happy—the bank is happy; the customer is happy—but we never get to really find the criminals?
Anthony Browne: Anyone who breaks the law should face the full force of the law and we want—

Q256 Chair: Yes. Do you have figures for us, Mr Browne, of how many prosecutions?
Anthony Browne: We don't collect those figures. It would be a question for the police or the Crown Prosecution Service.

Q257 Chair: Do you have those figures?
Katy Worobec: Not the prosecution figures, no. However, as part of this context, I think it is worth noting that under the FFA UK we receive intelligence from all the banks in relation to the fraud that they are seeing. That is passed through our fraud intelligence sharing system to the National Fraud Intelligence Bureau. I think that is the best way in which it can then look at the whole picture and try to identify organised criminal networks and try to work through that. Unfortunately, the nature of this type of fraud tends to be high volume and low value. It can be very difficult to investigate every single case and be able to get a resolution, but what the National Fraud Intelligence Bureau can do is to look at the intelligence that comes in from our sector and from others, match it together and see what that shows in terms of organised criminal networks. I think that then gives the police at least some fighting chance of being able to go out and hit them where it hurts.

Q258 Mr Clappison: I am very interested in the question that the Chairman has just raised with you. In a way, you are the victim and the customer of the bank is a victim. Although the customer may be compensated or repaid, he or she will go through some anxiety, no doubt, and you do not like to see your systems being comprised. The figure you have given us for penetration of online accounts was £39 million. Is that right?
Katy Worobec: £39.6 million, yes.

Q259 Mr Clappison: I am curious that you seem to have so little knowledge of what happens to the people who have been carrying out this crime, because you are a victim. Has anybody been prosecuted to your knowledge?
Katy Worobec: Yes, certainly. It is worth mentioning also we have our own dedicated cheque and plastic crime unit, which is sponsored by the banking industry. Although e-crime is not its particular specialism, it is dealing all the time with these types of frauds, so it is constantly bringing—

Q260 Mr Clappison: On the penetration of people's online accounts—many people obviously have online banking accounts—are you aware of anybody at all who has been prosecuted for that offence in this country?
Katy Worobec: Yes, there have been prosecutions. What we don't have is a set of figures that I can give you. For example, the Metropolitan Police e crime unit has done a sterling job in terms of dealing with this type of fraud.

Q261 Mr Clappison: Were the people who were prosecuted in this country or somewhere else?
Katy Worobec: A mixture, I think it would be fair to say.

Q262 Chris Ruane: My question leads directly on from that. Could we have the statistics on the balance of cybercrimes committed from within the UK and outside the UK?
Chair: Who would give us those figures?
Katy Worobec: I can tell you approximately how much fraud we see on UK cards. For example, if I look at the split for e-commerce—so fraud on UK cards spent online—it is about 70% in the UK and 30% overseas. That is where we see the spend going.

Q263 Chris Ruane: For that 30% overseas, we heard of Russia and eastern Europe before. Is that the case or is it just not the case?
Katy Worobec: Just to be clear, this is where the card details are used fraudulently. So the card details may be compromised in any number of ways and then used to purchase goods from overseas. For example, airline tickets is a fairly standard area where card fraud is spent overseas.

Q264 Chris Ruane: If it is eastern Europe and Russia or wherever, is there co-operation, or is there a league table of co-operation from those authorities? Do those Governments view it as serious, or do they think that it is just happening in the UK so it is not a concern of theirs? How much concern and co-operation is there abroad?
Katy Worobec: From the work that we do with law enforcement—we work very closely with our own police unit and other forces and the emerging National Crime Agency—I think it is fair to say it is patchy.

Q265 Chris Ruane: Patchy where.
Katy Worobec: In other words, there isn't a consistent approach in terms of response from other countries in dealing with fraud. Our own DCPCU has just set up, with funding from the EU, a joint team with authorities in Romania, because there have been some specific concerns around fraud in that area. It is trying to build some good relations with that country, as an example, but it does seem to be rather hit and miss in terms of the co-operation that you get from other countries in Europe and beyond.
Anthony Browne: One of the things we said in our submission to you is that we would like the highest international co-operation possible on this issue because it is an international issue, both at the EU level and globally.

Q266 Chair: Your main international organisation is Europol, is it?
Anthony Browne: That we deal with.
Katy Worobec: Yes, from the law enforcement perspective, but we look at it also from our perspective through the international card schemes—so Visa and MasterCard—because they obviously have an international footprint.

Q267 Chair: Of course. However, with the main policing unit, would you have a direct link to Rob Wainwright or his colleagues in Europol, or do you go through the Metropolitan Police and they then go through Europol?
Katy Worobec: I think we have to go through the Serious Organised Crime Agency at the moment.

Q268 Chair: So you go through what will become the National Crime Agency.
Katy Worobec: Indeed.

Q269 Chair: Are those structures okay? Is it working, or could it be a little bit more streamlined?
Katy Worobec: I think it could be more streamlined. What I mean by that is that I think we should look at ways in which intelligence can be better shared between law enforcement and the private sector—the banking industry. If we can get two-way information sharing—I think someone spoke earlier about trying to get better data sharing between countries—I think we could improve the situation a lot.

Q270 Chair: On a practical basis, if this happens at 5 pm on a Friday and you have uncovered some great fraud being committed and you pick up a phone, is there somebody there or have they gone home? Is this a 24/7 operation that you can deal with?
Katy Worobec: In terms of the banking industry, we would find that most banks often have footprints in other countries anyway.

Q271 Chair: No, not the banks. I am talking about the policing.
Katy Worobec: Right, okay. In terms of our own police unit, obviously we have a link into that. As far as more general policing is concerned, we would tend to go through our DCPC unit.

Q272 Chair: No, I understand that. Is it 24/7 or at 5 pm on a Friday does it all close down? Your system obviously carries on.
Katy Worobec: Are you talking about the banking side?
Chair: Not the banking side. When you ring up the police, or whoever you ring up, and you say, "Somebody is now emptying all these bank accounts," or, "This card has been fraudulently used and we want to stop it," is there somebody at the other end of the phone at 5.05 pm on a Friday?
Katy Worobec: There certainly would be in the DCPCU, yes.

Q273 Chair: What does DCPCU mean, for the purposes of the record?
Katy Worobec: Dedicated cheque and plastic crime unit.

Q274 Chair: Where is it based?
Katy Worobec: It is based in London. It is fully sponsored by the banking industry. It is a mix of City and Met officers working with banking industry investigators and support officers.

Q275 Chair: Good. We had not heard of that before, I think, so it is always nice to hear about new organisations. So they are there at 5.05 pm on a Friday?
Katy Worobec: They certainly are.

Q276 Chair: What about 10.00 am on a Sunday?
Katy Worobec: There will certainly be somebody available at 10.00 am on a Sunday, or me on my mobile, so yes.

Q277 Mr Winnick: That is reassuring.
Ms Worobec, you sent a letter to us, I think in February this year, and you cited a customer survey by Which? as demonstrating that the vast majority of customers are refunded quickly—within one week. However, it does appear to be the case that 29% of customers surveyed had to wait longer, in some instances as long as six months. What is your comment on that?
Katy Worobec: Our statistics show that 98% of fraud claims are refunded. We have done some work since that Which? survey—talking to our members—and 96% to 98% are actually refunded either the same day or the following day.

Q278 Mr Winnick: Sorry, I am getting confused. Which? says that 29% of customers had to wait longer, some up to six months. Are you disputing this? Leave aside the 2% for the moment.
Katy Worobec: Yes. Our members are telling us that between 96% and 98% are actually refunded the same day or the following day.

Q279 Mr Winnick: Who is telling you?
Katy Worobec: These are our members, which will be the retail banks and card issuers in the UK.

Q280 Mr Winnick: Should we have more confidence in them or in Which?
Katy Worobec: You have to look at the fact that Which? has done a survey asking people who have experienced fraud over the last five years what their experience is. There could be all sorts of reasons behind the apparent delays, and it would be interesting to understand a bit more about what the details behind the survey show us. I am not convinced that it necessarily conveys the accuracy of the situation, whereas our members have told us that these are the figures that they are seeing.

Q281 Mr Winnick: For the sake of argument, say the situation has changed or Which? could have been wrong in the beginning, what percentage of customers would you say have to wait if not for six months,

certainly, then beyond three months? Do you want to give a figure?
Katy Worobec: I think it is a very small number. It is in between 4% and 2% really and I think it will be at the lower end of the scale, so most will be resolved in a few weeks. Where lengthy and complex investigations are required, it may take some more time to get that sorted. However, they are few and far between, quite honestly.

Q282 Mr Winnick: I have great hesitation in challenging any witness, and I do not have any evidence to do so. Without in any way questioning your integrity, do you think it is possible to send some documentation—if the Chair agrees—to back up what you have just said?
Katy Worobec: I am happy to put these figures in writing to you, certainly.

Q283 Mr Winnick: With some evidence of what they are based on.
Katy Worobec: Yes.

Q284 Mr Winnick: It said that 98%—in fact you have just mentioned it—of those surveyed had their claims repaid in the end. Let us consider these 2%. On the basis that it is said that 94% of the UK adult population now own a credit or debit card, if the maths are right, this works out at somewhere in the region of 380,000 people a year. It is quite a large number of people, isn't it, that 2%?
Katy Worobec: I am not disputing your maths at all. I think it is worth bearing in mind that 9.9 billion card transactions take place every year, so we should look at this in the context of that. There will always be a small number of cases where things need further investigation. These cases can be quite complex and do take some time to resolve and, frankly, there are fraudulent claims made as well. So first-party fraud does play into the mix of the 2% that are not refunded as well. We must remember that.

Q285 Mr Winnick: Recognising that fraud needs to be investigated, we would be very simplistic and naive not to recognise that there are people who are not genuine, to say the least. Nevertheless, you would accept that people who have genuinely been the subject of such fraud should not be in a position where they lose out.
Katy Worobec: Absolutely. There will always be cases when unfortunately things are perhaps not handled as well as they should be. I am not saying there is 100% success in that space, but I do think the figures stand for themselves in terms of the overall approach to that particular issue of refunds.

Q286 Mr Winnick: Yes, and you are going to send us the documentation. Mr Browne, of course, you are the chief executive of the British Bankers' Association. Is the status of bankers high?
Anthony Browne: No. One of the joys of this job is I get sent all the information when the pollsters ask the public what they think about banks, and it is—

Q287 Mr Winnick: Are they lower than MPs and estate agents?
Anthony Browne: I don't know quite where they stand compared with MPs or estate agents, but they are about as low as you can get.

Q288 Mr Winnick: Before I ask you anything else, I come from a generation in which, despite my politics, and whatever may have happened in some other countries—certainly in the 1930s banks collapsed very rapidly in the United States, and there was depression and all the rest of it, not confined to the United States—in the main, in the immediate post-war period, one did have a feeling that nothing could be safer than to have your money in the bank. I am referring to British banks. That feeling of security and confidence has changed, hasn't it?
Anthony Browne: I can provide you with third-party polling data on this. If you look at the confidence that people have in the banking system, it certainly took a big hit after 2007—this might be slightly different from the angle you are taking—after the run on Northern Rock, but that confidence has largely returned. People do believe now that their banks are safe. I know this is not the subject of this session, but there have been a huge number of reforms in place to make sure that banks do not fail again.

Q289 Mr Winnick: So why the feeling that the surveys show, as you readily admit—
Anthony Browne: They are not generally to do with the safety of banks; it is the disquiet that the public have. In fact YouGov has a very big poll about this out tomorrow, which I think will be in tomorrow's papers. It is not the safety of banks that people are worried about. It is more concerns about mis-selling, the behaviour of bankers and remuneration—all the things that you debate regularly in Parliament.
In the polling evidence—and I urge you to look at this YouGov thing—concern about being victims of fraud really does not register in terms of people's concerns about banks. There are a lot of other issues that—

Q290 Mr Winnick: There is a lot for the banks to worry about.
Anthony Browne: There is, but actually fraud is not one of them. As you have been saying, 98% of people who are defrauded get refunded. I didn't quite understand the maths you set out earlier, but certainly the number of people who don't get a refund is going to be comparatively small.

Q291 Mr Winnick: Mr Browne, in this survey of Which? to which I referred, Halifax and Barclays were found to have the worst performances, with 34% and 39% of customers experiencing delays. Do you have any comments on that?
Anthony Browne: Unfortunately, I can't talk about individual members. One of the problems banks have had, and one of the reasons why the opinion of the banks is low, is because, in the words of Stephen Hester, they lost sight of the customer. The banks are determined to make sure that customers are treated properly, and fraud is an example of that. They have spent a huge amount of time and effort making sure

that customers are treated well. Any complaint and any dissatisfaction is a complaint too many, but the overwhelming majority of people do get their money back promptly. That is not being complacent. They clearly need to raise their game when there is dissatisfaction.

Q292 Mr Winnick: In your role as chief executive of the British Bankers' Association, do you take these matters up with individual banks? Which? obviously has high standing.
Anthony Browne: It does. I have a great regard for Which? and it does a lot of very good work representing the views of customers. In fact, one of the things I have done at the BBA is to set up a consumer panel to make sure we get full input from consumer groups into our policy-making work to make sure we can properly address their concerns. To answer your direct question, I have taken up individual matters of concern with individual banks.

Q293 Mr Winnick: Of course this is related to the direct inquiry we are having into e-crime. If people who feel that they have been the subject of fraud have sufficient confidence in the banks they are dealing with, it certainly helps the customer to have the feeling that the matter will be dealt with pretty swiftly and in a competent manner.
Anthony Browne: The banks are obliged to deal with it quickly. Under the payment services regulations, they have to give an immediate refund when there is an unauthorised transaction. There is a lot of detailed FSA guidance about exactly what that means, which we can talk about if you want. That is certainly the standard to which the banks work. If people are not satisfied, they can take their complaint to the Financial Services Ombudsman. I know you had a previous witness who gave evidence about this, and there are something like 70 complaints a week.

Q294 Chair: Mr Winnick has rightly raised this point and he has rightly raised the Which? report. There is a big difference, is there not, Mr Browne, between a bank like First Direct, where 83% of customers were reimbursed immediately, and Halifax which has a figure of 64%, and Barclays where only 59% were reimbursed? You have seen this survey, presumably.
Anthony Browne: I have, yes.

Q295 Chair: How do you account for the difference between this? It is a very large figure, isn't it? I should declare my interest: First Direct is my bank.
Anthony Browne: It has a good reputation. Exactly what the banks should do, as I say, is set down in legislation and there is guidance behind it.

Q296 Chair: Yes, but they are not doing it, are they?
Anthony Browne: The point is then that each individual bank has different protocols about how they precisely deal with it. Katy would be far closer to the detail of that than I am.

Q297 Chair: What do we do about this huge difference that Mr Winnick has highlighted: 83% for First Direct; 59% for Barclays?
Katy Worobec: I think the difficulty is with the survey that Which? has run. It is looking at people who have been claiming fraud refunds over the last five years, and the impact of the payment services regulations has really bitten in the last few years. It may be that some of these have perhaps experienced a fraud in the first part of that. So we may have seen an improvement in performance, and I think we probably would do in the recent past. As I say, I think it is very difficult if I experienced fraud five years ago to remember exactly what time scale it took to get my money back. There is an element of not really being able to get behind the figures and see exactly how the questions were asked and so forth. For example, it may be that some of the respondents did not confirm the fraud immediately it happened on their account. It may have started as an unauthorised transaction or a dispute, and then been confirmed as fraud later. That may have been part of the delay, for example. So I think there are lots of reasons behind that.

Q298 Chris Ruane: What are banks and card providers proactively doing to raise customer awareness about keeping their financial details secure online?
Katy Worobec: At Financial Fraud Action UK, we have done a fair bit of work in the last 12 months in this space. It is something that we are very much concerned with. We have been working with the National Fraud Authority as well. In the earlier panel you were talking about targeted customer education and focusing on particular at-risk groups. We have been working the National Fraud Authority, and I can give several examples. One was a campaign called "The Devil's in your Details" that had two aspects to it. One was targeting young people, and it did make use of a viral campaign on YouTube to get the messages through to that section of the public about looking after their details and how important it was. A second aspect of the campaign was targeted at middle-aged ladies using the internet.
At the other end of the scale, we have also done some work with elderly and vulnerable people in Durham—as a pilot initially—where we went out and interacted with their network. So, going to coffee mornings, citizens advice bureaux and libraries—those sorts of things—and getting information out in a face-to-face way, which resonates with that particular group of people. There was a range of different activities. "The Devil's in your Details" campaign that we ran was a collaboration between the National Fraud Authority, the banking industry and the telecoms industry, so it was getting a joint and consistent message out about protecting personal information, jointly funded by those three sectors.

Q299 Dr Huppert: A question for Katy Worobec. There has been an interesting exchange of letters. I think you know of my constituents, Steven Murdoch and Ross Anderson, who have done some very interesting work on how chip and PIN cards can be compromised without actually knowing the PIN.
Mr Winnick: A bit of name calling.
Dr Huppert: There have been some fairly strong words. Professor Anderson has given evidence to this

Committee, which I think led to your letters. First, do you accept that it is possible for somebody to have their chip and PIN used, and it looks like there was a PIN even though they did not divulge that PIN?

Katy Worobec: We are aware of Ross Anderson's research and Ross and his team do a lot of good work in that space. On the demonstration that they made in terms of that particular vulnerability in chip and PIN, we are not saying it is not possible to do that. What we are asserting is that it is quite a complex and difficult way of committing fraud, and we are aware that there are much easier ways, unfortunately, for the fraudster to commit fraud. The type of attack that Professor Anderson was talking about relies on the fact that you need to have a physical card from the cardholder. If the cardholder reports that card lost or stolen, the fraud is blocked. That is quite different, for example, from the skimming of mag stripes, which is the problem that we have countered by introducing chip and PIN, where they would have been able to copy the magnetic stripe of a card and then create a large number of cards that cloned that original card without even taking it away from the cardholder. So that had much more potential for the fraudster being able to commit fraud on an industrial scale. As I say, we are not saying chip and PIN is 100% secure, but it does offer a much more secure platform on which to work than the old magnetic stripe cards did.

Q300 Dr Huppert: Nonetheless, it means that there is a possibility that people who claim that money was taken from them fraudulently—they claim they did not divulge their PIN, yet the suggestion is made that they must have done so—are right. Indeed, in 2012, there were 64,000 complaints to the Financial Ombudsman Service about banking and credit, and 54% of those for credit cards were found against the bank. There are various similar figures. Do you think that the number of disputed chip and PIN cases that have been referred to the Ombudsman suggest that there may well be genuine cases where it is falsely suggested that people may have colluded or been insufficiently secure with their PIN?

Katy Worobec: I really don't believe that the cases where the use of a PIN cited are down to the sorts of attack that Professor Anderson was talking about in his research. I think there are easier ways to defraud the system, as I have said. I would assert that it is unlikely, in fact, that the bank will simply reject a claim for a refund just because the legitimate PIN was used. They will look at a number of factors and criteria before making a decision about whether a claim is refunded or not.

Q301 Dr Huppert: Professor Anderson has given some specific examples, but if you say it is not really likely to be used because there are easier ways of fraud, why did you ask Computer Labs to remove the paper that it published from the internet?

Katy Worobec: We were concerned that some of the information there might be giving information away to potential fraudsters. By describing it in the level of detail that they did in the paper, it might have encouraged people to try doing that. So we were concerned that it was not a particularly good way of talking about that particular type of fraud. What we would have preferred is for Professor Anderson to come and talk to us about it and then we could have seen whether there are things that need to be done. However, to publish a lot of detail on the internet does tend to encourage people to try that type of fraud.

Q302 Dr Huppert: It was circulated among a number of the banking community and he highlighted it well before it was published. Surely the correct thing to do is try to fix the problem rather than asking people not to reveal the fact that it exists. A question for Mr Allen: what work is being done to try to fix the chip and PIN technology problem? From reading the paper, it is clear that it is entirely fixable. You could update the protocol so that this particular hole does not exist any more.

Anthony Browne: Can I highlight some points here? One, and it comes back to several of the questions here, is that the banks have immense financial interest to reduce fraud. With 98% of fraud victims being refunded, it is a direct cost to their bottom line, which is why they spend a huge amount of money on combatting fraud and on various publicity campaigns—

Q303 Dr Huppert: Unless you can insist that it is the cardholder's fault, in which case you do not have to reimburse them.

Anthony Browne: There are a lot of new technologies coming in the whole time, and Katy has a lot of the details, which have been very successful in reducing the amount of fraud. The reason why fraud went down to a 10-year low, despite a massive increase in cyber online accounts and everything else, is because of all these new technological investments that have made it far more difficult to commit fraud. Obviously it is not perfect. It is questionable whether any system is ever capable of being perfect, but the banks are spending huge amounts of effort to combat it. Sorry, you asked a question of Matt and I interrupted.

Matthew Allen: In response to the question, banks are constantly updating their systems and controls, and this is a constant challenge. We outlined in our submission to the Committee that this is a highly mobile threat. It is rapidly evolving, so banks are very vigilant.

I would also add that there is significant action at the firm level. At the industry level and at the firm level, we are constantly working with our members—both at the BBA and in partnership with FFA UK, to make sure that we can provide the best possible service to our members in terms of highlighting new emerging trends. I can give some examples of the work we have done in this area. You mentioned Europol earlier. We have been engaging with Europol. I took a delegation of five banks to Europol in October. Europol has recently visited the BBA. That is entirely to try to find ways to promote a stronger dialogue between law enforcement, at the international level, with the banking sector. We have knowledge in the banking sector of emerging crime techniques and so do law enforcement, so we are certainly very keen to promote that dialogue. There is significant work by individual firms, but there is also quite a lot of work at the industry level as well.

Q304 Steve McCabe: I think my question follows on from this. I do not think anyone disputes that there is a huge effort and a significant amount of investment in trying to counter online fraud. Despite that, it does seem to be on the rise and there is a huge amount of money being stolen each year. Is that because this is the sort of crime where the number of criminals and victims are just expanding, or is it because some of the security systems are pretty poor and inefficient?

Anthony Browne: Can I just come back to the point, Mr McCabe, that there is a huge amount of money and any fraud is too much fraud? However, banking is 8% of GDP and it is 1% of fraud in the UK, so it has a far better record than the rest of the economy. That is not to be complacent but there is—

Q305 Steve McCabe: Most people would regard this as a relatively new form of crime, so we may still be in the early stages.

Anthony Browne: Yes.

Katy Worobec: I would like to talk about something that we have seen recently. In terms of the types of attacks that we are seeing from fraudsters, it does tend to be focusing on the customer and trying to dupe them into giving away personal details and security details. There is a particular type of insidious fraud that we have been seeing in the last year. We refer to it as "courier fraud". Essentially, particularly elderly and vulnerable customers are targeted by someone who phones up claiming to be from their bank or from the police and says, "There has been fraud on your account. We need your PIN number, we need your card, and we need evidence of what you bought. Please give it to the person who comes to the door," and they give their details away.

In a similar vein, there is a constant attack from fraudsters to try to get people to give their personal details away. That seems to be where the attacks are coming from at the moment. In a way, it is less about the security of the systems, particularly the online banking system—it is robust—and what it is is that, unfortunately, the customer is being duped into giving their details away.

Q306 Steve McCabe: Banks do phone customers and invite them to give personal details over the phone. That is not unusual, is it?

Katy Worobec: The sorts of details that you would be asked as part of the "know your customer" details. Banks are required to identify a customer when they phone them up for whatever reason. Unfortunately, they are asking what look like personal details, but they are very limited. We are talking about a situation where people are being asked to give their PINs and their cards away.

Q307 Steve McCabe: I do not want to interrupt you, but if the message to the elderly person or the vulnerable person is, "You should not be duped and you shouldn't give over this personal information to these people who are fishing for your details," the very fact that the bank itself asks for personal details is likely to lead to a degree of confusion in the mind of that person, surely.

Katy Worobec: I do understand what you are saying. Unfortunately, the bank is required to do that in order to identify the customer. It is one of these vicious circles. What we do say in terms of advice to customers is if they are at all concerned about who they think they are speaking to, they should put the phone down and dial the phone number that is on the statement or on the website and speak to somebody. So they go back into the system if they are at all concerned about anybody they are speaking to, which I think is the best piece of advice that we can give.

Anthony Browne: It is obviously different if you are phoning a bank, in terms of telephone banking, and they ask you to prove your identity when you are phoning them, as opposed to the bank phoning individuals, which is far rarer.

Q308 Steve McCabe: Should I deduce from what you said that you are satisfied that these security systems you have are adequate and that no criticism can be made against them, or would that be a wrong assumption? I just wondered, because you dealt with only the second part.

Katy Worobec: I wanted to give an example because I think it demonstrates in a way that the bank systems are robust. That is what is forcing the criminals to target the consumer as the weakest point, and that is really where I was coming from.

Chair: Excellent. Thank you very much for your evidence. It has been most helpful and we will be no doubt writing to you. I know you have promised us some documentation. We would be most grateful if it could be sent as soon as possible, because we are about to conclude our report.

Tuesday 23 April 2013

Members present:

Keith Vaz (Chair)

Nicola Blackwood
Michael Ellis
Dr Julian Huppert
Steve McCabe
Mark Reckless
Chris Ruane
Mr David Winnick

Examination of Witnesses

Witnesses: **Art Coviello**, Executive Chairman, RSA, The Security Division of EMC^2, **Professor Jim Norton**, Engineering the Future, and **Ilias Chantzos**, Senior Director, Government Affairs for EMEA and APJ, Symantec, gave evidence.

Q309 Chair: I call the Committee to order. This is the penultimate session of our inquiry into cyber and e-crime. After this session, we only have the Minister to take evidence from. I welcome the witnesses to the dais, and thank you for coming here from a very far distance. I know, Mr Coviello, you in particular are not a frequent visitor to the United Kingdom, so we are glad to have you here.

Art Coviello: Thank you.

Chair: There will be a Division in the House at 3.05pm, so we are hoping to finish your evidence by then so you do not have to wait for us to come back after the vote. May I start with you, Mr Coviello. Obviously, we will go on to talk about fraud and banking crime and cybercrime in general, but with the background of the Boston bombings that took place just 10 days ago, I know your company deals primarily with financial issues. Have you ever been asked by the Government of the United States or any other Government actually to monitor websites in respect of dealing with terrorism?

Art Coviello: No, that is not something we would engage in, although our security products and services extend well beyond the financial sector itself, including protecting the Government.

Q310 Chair: Given that you look at these websites every day and you have a large team of people, which I understand is in Israel—

Art Coviello: Yes.

Chair:—who do the monitoring of these websites, would it be too much of an extension of what you do to actually monitor these other websites that are causing concern to the security services?

Art Coviello: It probably would be. I think we could, but those types of activities would tend to be handled by the Government and not by us. We restrict ourselves to things of more of a commercial nature.

Q311 Chair: Now, we have had evidence that has been given to us by the head of the City of London Police—the City of London Police in the UK deal with cybercrime—who told this Committee, and I quote, “We are not winning the war on online criminals”. Do you think that the war has been lost?

Art Coviello: I do not think the war has been lost, but we are not winning it either. I think what people need to keep in mind is not so much the threat—obviously, we have to keep in mind the threat environment—but what people sometimes overlook is what I call the expansion of the attack surface. We have now developed so many web applications, we have so many remote access devices, mobile devices, we have so many points of entry into our enterprise, and now we starting to outsource a lot of our infrastructure and applications to the cloud, that we have expanded the attack surface and made it literally easier for the attackers to take advantage of us. But having said that, I am a technologist, so I am an optimist, and I believe we can win the war, but we are not winning it yet.

Ilias Chantzos: If I were to address the question, let’s say, in a lighter fashion, I would say that if we had lost the war things would not be working very well right now, would they? It seems to me that things are actually still working quite well. We can go online to the bank. We can order online tickets. We do order online goods. The digital economy seems to be operating and it seems to be operating quite well and people trust it. This is not a question of winning or just losing a war, but of understanding that security is a moving target, security is a moving goal. The technologies change. We see an expansion in cloud. We see an expansion in mobility. As the technologies change, the attack surface changes, the techniques that the attackers are going to use change. What is important is that we adjust ourselves and follow that moving target in order to achieve that objective. We will never have 100% security.

Professor Norton: I do not believe that we are losing the war. It is a war we can win, but we will not win it purely with technology. There are three things we have to do, and the first and most important relates to people. I could build you the most perfect security system, as I am sure could my colleagues here, and I am sure a thoroughly misunderstanding user of that system could defeat it. We do not educate our people properly. We do not train them in what is good practice, and there is not a technological solution to that. So, one, we need training; two, we need better software, and we know how to write software very much better than we actually do in practice in most cases today; and thirdly, we need better resourcing for the police. That is not just nationally but internationally.

Q312 Chair: Mr Coviello, I am concerned at the number of social media sites or internet sites that offer people packages for fraud on the internet as part of

internet services. Do you know whether there are any well-known social media sites that have been used for that purpose?
Art Coviello: As a matter of fact, recently—and I think we are going to release the coverage this week—an Indonesian hacker was actually using Facebook as a means to disseminate information about his fraud as a service. That was, quite frankly, very unusual but it is a disturbing change to anything we have seen previously. It just suggests an utter disrespect of being caught.

Q313 Chair: Has that stopped, do you know?
Art Coviello: I am sorry?
Chair: Is it still ongoing on Facebook that people can—
Art Coviello: I do not know if the site has been brought down as yet. I am assuming that it will be brought down quite shortly.

Q314 Chair: I do not know whether you all have seen the survey that has just been published by Verizon, which shows that state-sponsored industrial espionage is now the second most common form of cybercrime. Have you all seen that survey? It has just been published today. Is it a surprise to you that there is so much state-sponsored espionage, and, if so, do you have any indication of which countries are doing this? We have had a list from the City of London Police. They have talked about Russia and the Eastern European states, but do you know which states might be responsible?
Art Coviello: One of the problems with any attack is attribution, being able to trace the attack back to its source. That is where people have to be very careful because unless you have evidence, to point the finger at a particular nation is clearly not the right thing to do, and I see too much of that. Having said that, given the level of sophistication that we see in attacks, it can only be sponsored by nation states. We see it clearly. We see it in the form of economic espionage. It is ongoing, and it is increasing.

Q315 Chair: Thank you. Just one final thing: could you confirm the Norton study, which shows that there are 556 million victims of cybercrime every year—is that a figure that you recognise? Also, the cost of cybercrime to the UK at £1.8 billion. Do you have any fresh figures or are those figures that you can endorse?
Ilias Chantzos: I believe the Norton study that you are quoting is the latest study that has been released from us until now. We have actually released very recently the *Internet Security Threat Report*, which is the latest statistics that we have analysed for activities in 2012, which are not focused on the consumer side only. Having said that, I should emphasise that the methodology of the Norton study is such that the results of the study are based on self-reporting. We went out and asked individuals whether they had been victimised. It is not based so much on attacks that we have actually observed but rather on what the public has told us. The numbers in terms of financial losses is based on the numbers that the victims claim that they have lost.
Chair: Sure.

Q316 Mr Winnick: RSA apparently suffered a serious security breach, which has been dealt with. In fact, the company has been commended for its response. Was that the first major security breach?
Art Coviello: In terms of RSA, clearly it was, yes.

Q317 Mr Winnick: What did it involve?
Art Coviello: It was a very sophisticated attack. It was two separate APT groups, as we define them; advanced persistent threat groups. Again, one of the things we did was immediately contact law enforcement and request additional help from the National Security Agency as well as from Homeland Security. The Government responded very quickly in helping us understand—

Q318 Mr Winnick: About what time was this?
Art Coviello: The attack commenced on March 4th, 2011, and within two days they were on-site helping us. These kinds of attacks are very difficult for a number of reasons. You have to ensure that you find all the places where they have compromised your infrastructure before you take them out because you do not want to tip them off that you know that they are in there. This is the kind of help and assistance that was provided by the Government. Of course, we have our own capabilities. Fortunately, while we were not able to stop them from exfiltrating some important information from our infrastructure, because we discovered the attack timely enough and disclosed the attack timely enough, there were no losses sustained by any company as a result of the attack.
Mr Winnick: I see.
Art Coviello: But I should add that it was the first time that law enforcement had seen two separate groups attacking a company at the same time. Again, the sophistication of the attack could only have been carried out by a nation state based on our point of view and that of law enforcement. Another interesting aspect of this is that the attack commenced at a supplier of ours. Emails from that supplier, targeted emails, were sent into our employees, and that is how they were able to breach our perimeter. Also, we were not the ultimate victim of the attack. What they wanted to do was use the first company to get to us, and ultimately, in our point of view, they were after our defence industrial base. They were going to use our information to attack our defence industrial base and potentially our Government.

Q319 Mr Winnick: Do you think lessons can be learnt by other companies from the manner in which you dealt with this and the support that was given, as you say, by the authorities?
Art Coviello: Well, yes. I believe that any company who is breached, which could potentially result in harm to another company, has a moral if not legal obligation to disclose that breach so that they can prevent other companies from being hurt, and that is exactly what we did.

Q320 Dr Huppert: Can we step back for a second to this issue of what we should aspire to? Mr Chantzos, I think you said that we cannot have 100% security, and, Professor Norton, you made the point that a lot of it is about behaviour and what information there is. To what extent would you subscribe to the principle that if people put data out online in the broader sense it is fundamentally vulnerable, and so if you want to make data safe, you do not collect it, you do not put it out there? Would you accept that as a principle?

Ilias Chantzos: Well, I think it is very important to understand the value of our personal data. Most people do not appreciate the importance that our personal data has and, frankly, you see whole lives, whole lifelines, timelines, on social networks. That is extremely dangerous. The reason why it is extremely dangerous is that, to follow up on the points that Mr Coviello so accurately described, you launch a targeted attack—and by the way if you look at the *Internet Security Threat Report* that we just released, we have seen a 42% increase in targeted attacks—by targeting the individuals. How do you target the individuals? You profile them. The fact that you have your lifecycle of friends, your information about yourself on a social network publicly visibly available, makes them a perfect open-source intelligence tool, and makes it very, very easy for you to be profiled, followed, and then attacked.

One of the most frequent examples that I give is people put their birthdays on social networks and then they accept congratulations on their birthdays, but, by the way, that is one of the three to four authentication questions every time you call your credit card company. What is your date of birth? Yet this is an example of how it can go terribly wrong. Professor Norton was correct in saying that security is not just about the technology, it is also about the people and the process, and this is exactly why there are the social network problems that we see.

Dr Huppert: I was hoping for more of a yes or no, but thank you for that anyway.

Professor Norton: May I just add to that a little? In an information economy personal information is now traded as value. That is fine if the person whose information is traded is doing that knowingly, but we have, I am afraid, miserably failed, not just here but probably around the world, in educating people about the impact of that. Yet we are trading information as value not just on social media sites but in all sorts of other ways as well without a true understanding by the individuals concerned of its implications.

Q321 Dr Huppert: But just in terms of the principle that I was trying to outline, you would broadly agree with it or broadly disagree that if you really want to avoid data loss, you do not make the data available?

Professor Norton: No.

Q322 Dr Huppert: You disagree?

Art Coviello: Absolutely.

Professor Norton: There is a hierarchy of data, and it is very important that people are trained to understand that. There is some data you may want to release, and it may be greatly beneficial to you to release. There are others you do not want to release. I think simply treating it as inaccessible is wrong.

Ilias Chantzos: You have to effectively risk-manage the type of information you release about yourself.

Q323 Dr Huppert: I am being prompted to ask about some other issues. Professor Norton, you said something about poor software design being a big problem.

Professor Norton: Yes.

Dr Huppert: I used to write a bit of Perl script, so I am probably responsible for much of this. Why do you think the security is so poor, and what do we need to do in order to get standards higher in terms of the software that is being produced so that it does not have injection holes and all sorts of things?

Professor Norton: We do not use the formal mathematical methods that we have available, which we have had for 40 years, to produce better software.

Q324 Dr Huppert: Are they applicable to all complex software, though?

Professor Norton: Any piece of complex software can be decomposed into pieces of less complex software. However, you are right, it is much more of a challenge if you are writing a global operating system, but much of what we do, and I am thinking here, for example, of infrastructure, are actually very simple systems, and they are entirely amenable to being written with formal methods. What I am getting at there is that we have a culture in the software industry of testing. Testing will only prove what faults you have; it will not tell you what you have not found. It would be far better to have a culture of better design, which is designing out the faults before you have to test them out, which is impossible anyway.

Q325 Dr Huppert: Is that something that could be done easily, or do people have to be specially trained? I have never tried formal methods myself, so I do not know how easy it is.

Professor Norton: The National Security Agency in the States has pioneered the use of this in a thing called AdaCore. They demonstrated that it could be done at a very comparable cost to writing less good software. It is a matter of habit. Our universities used to train in it, but the industry did not hire the people who were trained, so they stopped giving the courses in it. This is a Catch-22 situation we need to resolve.

Q326 Dr Huppert: Mr Chantzos, I think Symantec said that providers will only be willing to accept liability for their products if they get control over the way in which consumers use them. Is that right? Do you think that slightly insulates companies from any responsibility?

Ilias Chantzos: I think you are perhaps reading more in there than what we have actually said. First of all, we already have liability under law for the stuff that we make within the marketplace. The question really is if we look into extending that liability, what is a reasonable level, and what is appropriate given the controls that the software manufacturer has or does not have on this product? As Professor Norton I think also admitted, there cannot be such thing as a perfect software. It is not possible right now. The issue is that we do not have an effective control of the way that our customers use the software that we make available. Should we be liable also for the fact that, for example, users take the software and do not patch it? You look around; systems get vulnerable and get attacked for malware that exists from 2008. The third most popular infection is Configure back in 2008, for instance. It is not as simple as saying there is defective software out there. It is also about how do the people install it and use it; is it fit for purpose for what it is being used for at the moment?

Q327 Nicola Blackwood: I just wanted to go back a little bit to follow up on the issue of the security breaches, which you were speaking about, Mr Coviello. You mentioned the fact that you think it is very important that organisations and institutions come forward when they have been breached but that many are reluctant to do so for reputational reasons. Now, I believe that you came forward in 2011 saying that you had been breached, but you mentioned the fact that the breach had occurred in 2004. Is that correct, or am I mistaken?
Art Coviello: No, mistaken.
Nicola Blackwood: Sorry, that is just the information that we have here.
Art Coviello: No, the breach occurred in 2011. We determined that information was taken around the 16th and we went public around the 17th, in that fast a timeframe, yes.

Q328 Nicola Blackwood: Do you think that other companies would do the same, or do you think that there is a general reluctance to do so?
Art Coviello: Well, I can only speak for my company, but obviously there is a fair amount of humiliation and embarrassment. In our case, it is our primary responsibility to protect our customers. It would be a total abdication of everything we stand for if we had not come forward and said there was a breach and give remedial advice to our customers to protect themselves.

Q329 Nicola Blackwood: Are you aware that the Government has brought forward a new cyber-security fusion cell in order to create an environment for companies and organisations to gather information and bring information forward in order to improve the gathering of information on such attacks?
Art Coviello: Yes.

Q330 Nicola Blackwood: Do you think that this will be helpful in these matters?
Art Coviello: Absolutely.

Q331 Nicola Blackwood: Why do you think it will be helpful?
Art Coviello: Because any opportunity you can timely share information about attacks, as long as you disseminate the information broadly, which is what our Department of Homeland Security did in our case, mans that all potentially affected companies can be on the lookout for a similar-type attack, whether it is the IP addresses from which the attack has been launched or the particular malware itself.

Q332 Nicola Blackwood: Do you think that there is anything they should be doing better with this particular cell? Do you have any advice for improving it?
Art Coviello: I am not deeply familiar with it, so I cannot give you such advice. I would say as a general statement the more you can do the better.

Q333 Nicola Blackwood: Did you have anything you wanted to add?
Ilias Chantzos: I do, actually. Very quickly, there are two different issues here. One is the question of information sharing, and the other one is the question of security breaches. You should be aware that already in the UK the ICO has encouraged the reporting on a voluntary basis of security breaches when personal data have been lost. I think that is very important and a step in the right direction, and I agree with Mr Coviello and his points about transparency and responsibility of the companies. I would also argue that that policy results in better security because nobody wants to be in a position where they have to go and report something that unpleasant. At the same time, you also need to be aware that this discussion is taking place in Brussels, so there will be legislation. It already exists for the telecoms, and it has been proposed for other policy areas as well.

Q334 Chris Ruane: To Art Coviello, you have said that the traditional models of security, such as using firewalls and antivirus software, are no longer effective against sophisticated online threats. What should companies do instead?
Art Coviello: In an age where the attack surface has broadened, as I pointed out earlier, in an age where there is no discernible perimeter, perimeter-oriented defences are less and less effective. So, the game shifts from outright prevention of breaches to early detection and response to breaches. The model that we advocate is one where you have technology that can detect these breaches far more timely. To do that, you have to have a lot of data. You have to be able to see the faint signal from the attacker that anomalous behaviour or anomalous flow or use of data is occurring. To do that requires a substantial capability to correlate and analyse vast streams of data at very fast speeds.

Q335 Chris Ruane: Okay. This is to all of you. We understand that the Zeus Trojan, the malware most widely used by criminals to target financial institutions, is detected less than 40% of the time by antivirus software. Does this indicate that the antivirus software is no longer fit for purpose? Is our technology—the good guys' technology, the good guys' brains—better than the bad guys'?
Ilias Chantzos: I would like to actually see those detection statistics, but I would begin by saying that, first of all, we need to bear it in mind that the traditional antivirus technology, meaning the signature-based detection, is by no means any more sufficient. Why? Because it is based on the premise that I will see the virus, I will capture it, analyse it, and therefore I can detect it. What we see right now is attackers using polymorphism, meaning techniques whereby they constantly mutate, to use a biological example, the virus so that it can be less easily

detectable by the antivirus software. Rather than focusing on the antivirus, modern-day security needs to focus on protecting the information in multiple layers by doing things like behavioural blocking, by doing things like intelligence analysis and by doing things like correlation, not just signature-based detection.

Chair: Professor Norton, you do not need to put up your hand.

Professor Norton: We are missing a huge resource here, and that resource is the people who work for us. You will probably have seen BIS published a report this morning that suggested that the vast majority of UK companies never bother to train their people in any kind of information security or the reasons why it is important. If they were so trained, you would be doing exactly the same thing as used to happen in the physical world. You would detect fraud in particular because you had a member of staff who would never go on holiday and so on. If people were sensitised to looking for unusual activity in the systems they use, we would have another entire line of detection here. Instead, we tend to regard the people who work for us as the enemy and the danger, not the people who could be helping.

Q336 Chris Ruane: How do you turn around that mindset?

Professor Norton: It is a major task in training, and it is not just for jobs; it is across the generations. You have to explain why this matters and why you have to treat those systems as if they were yours, not just your company's, and you care about it.

Art Coviello: I guess I have to respectfully disagree. While I believe fervently in defence in depth and while I believe fervently in educating our people in terms of policy, attackers today are far too sophisticated, and the average person is no match for the attacks. Now, could you prevent a small percentage of them if you had better training? Absolutely, but that is not going to get us there. Again, I would not say do not do it, but I would not expect a major return from it.

Ilias Chantzos: Mr Chairman, can I give a very simple, practical—

Chair: So long as it is very quick.

Ilias Chantzos: Very quick; think for a moment what the job of our HR colleagues, human resources, is. Their job is to do exactly what we are told on email not to do: receive emails from people they do not know and open attachments that say CVs, which can very easily contain malware. I am giving this as an example of how social engineering is actually easy despite perhaps the training that people will do. Still, training is important, no question about it.

Q337 Michael Ellis: Gentlemen, you have referred earlier to examples of individual responsibility for online security, and you used the birthday example—we all know people who tend to either use their birthdays as passwords or give them in social media and then get asked those sorts of questions by banks looking for authorisation. I notice, Professor Norton, that you used the Highway Code as an analogy for increasing the responsibility of individuals to keep their information secure online. What practical changes could be made, do you think, to increase responsibility in this area?

Professor Norton: At the risk of being boring, I am going to go back to education again. We do expect certain levels of behaviour of the people who drive on the road. In the various organisations I have been part of, the British Computer Society, where I was president, pioneered various elements of simple training in this area, and I think it is absolutely crucial. We released a series of technologies. I will give you an example. In Germany, when broadband internet was introduced, it came complete with antivirus packages. It was not sold without it. We did not do that here. We just let the technology out there without the help and support that people would need to use it safely. You would not dream of doing that with a car.

Michael Ellis: The problem is, as is so often the case with the internet, how would you enforce that? We know how we enforce rules of the road and other regulations, but how is it possible to enforce behaviour so that people are not cavalier with their own security and then introduce breaches?

Professor Norton: There is no simple solution to that, I have to concede, but I think the work that is going on in Government at the moment, for example, to throw out the teaching of information technology and bring in teaching of coding and computer science is a huge step forward. It should also include basic computer hygiene and security.

Q338 Michael Ellis: Mr Chantzos, do you have any observations to make further to that?

Ilias Chantzos: There is no doubt that education and people is a big component. Clearly, we are already doing a number of things like Get Safe Online, for example, or the child NGOs that exist in the UK and continue to engage them. At the same time, from the perspective of the provider, we try to offer security by creating more distance between the security and the user so that it is more invisible yet it works for the individual. The security becomes something that he does not need to modify or change. It does not become an obstruction; it becomes an enabler. Obviously, on the commercial side, try to make available security through the ISP to the end user through the OEM channel.

Q339 Michael Ellis: This is what I want to press you on, because isn't it up to people like yourselves and the companies to actually take some responsibility in this area rather than putting it on the individual and say, "We can develop technology that can do away possibly with passwords as we currently know them so people do not have to remember passwords and they are not so open to abuse or interception as we currently see them"? Is that not something that could be developed? Can we not improve this area?

Ilias Chantzos: It can be improved, but at the same time you need to bear in mind the kind of risk that you are going to have. For example, if we do do away with passwords and we use fingerprints, you cannot cut off your finger if you lose your fingerprint. As a user, you see the challenge.

Art Coviello: Once again, I think education is an admirable thing. I think personal responsibility is an admirable thing; we should encourage it. But the fact of the matter is the consumer-facing organisations are the place to solve this problem. Whether you should know it or not, 10 out of the top 11 UK banks use our risk-based authentication in online transactions. It is a technology that is seamless and transparent to the user. The software takes a device fingerprint of the device you log on from and it recognises you based on the geographic area of your IP address and certain characteristics of that device. We also have the capability in software to allow the bank to monitor your transactions looking for anomalies. The way security has to move is towards understanding anomalies in human behaviour, as I said earlier, and anomalies in the flow and use of data, and we can use technology to do that.

Q340 Michael Ellis: Recognising something that looks suspicious?

Art Coviello: Exactly.

Professor Norton: Let me emphasise the two points I made in my opening answer, and also say it is a question of better software. We should not have websites that are open to SQL attacks and things of that kind. We should do this much better. It is also down to better enforcement and a much better chance of getting caught.

Ilias Chantzos: And integrated.

Professor Norton: Yes.

Chair: Thank you very much.

Q341 Nicola Blackwood: I think in the course of this session we have heard a lot about the scale of the challenge and the pace of the threat as it changes. I think I heard from Professor Norton an emphasis on individual responsibility and at this end an emphasis on technological resilience. Can I have some kind of an assessment on how you think the private sector and the public sector—so, policing but also those who hold a huge amount of data such as perhaps the NHS and our schools—are working together at the moment and how we need to work on improving that, starting with Professor Norton, perhaps—

Professor Norton: Can I make a proposal, and that is—

Nicola Blackwood:—who still does not need to raise his hand to answer.

Professor Norton: It is a habit; absolutely. We have some interesting tools in the accounting world that we ought to be using. I am a chartered director and I am also the Chief External Examiner of the Institute of Directors. One thing we could do is cause the accounting profession to take much more seriously intangible assets, which are all those databases that you were mentioning. If they were valued on the balance sheet and if the board were to take a stonking great impairment write-down if they were lost or compromised, this issue would rise up the priority of boardrooms remarkably. That should apply equally in the public sector. The point is we have tools to do this; we are just not using them, and that is a great shame.

Ilias Chantzos: It is going to be a combination of policy; it is going to be a combination of technology, quite frankly. One of the biggest challenges that we see right now in information-sharing is the creation of the trust environment, the creation of the infrastructure to share that information, and very often as well we see challenges around legislation, data protection being one of them. I think it is critical, and I think the UK is a very good example of a country that is working in order to address all these issues, so bringing together public and private sector, finding mechanisms to exchange information and building an environment of trust. I think that a number of other European countries are trying to follow that example, but I think in the UK very good work is done in that direction.

Art Coviello: Once again, I have to disagree with my colleague. I actually started my career as a certified public accountant, and I think grossing up the balance sheet for some value of a database would be an extremely bureaucratic answer to a problem, so I would not advise it.

In terms of public/private partnership, in the US we have been talking about public/private partnerships since 2003, and we have got nowhere. Quite frankly, it is an extreme frustration. I do not know the details of how it is working over here, although just in general the outline of your strategy is far more coherent than anything that is being done in the US, I can tell you that. I can also tell you that it appears that you are on the right track around information sharing. Unfortunately, in the US we have not been able to get a Bill passed to facilitate information sharing, which to me is quite a pity. Anything that can be done to use Government as a clearing house to receive and disseminate information broadly about attacks is going to increase the effectiveness of our ability to detect and respond to attacks. If, as I said earlier, breaches are probable, if not inevitable, then having intelligence sooner as opposed to later is fundamental to building out a new model of security so that we can shrink the window of vulnerability from all attacks.

Q342 Chair: Thank you. Professor Norton, finally, you were not one of the nine cyber-security experts who wrote to *The Times* this week asking the Prime Minister to drop his proposed legislation. Is it because you do not agree with them or that you agree with the Government's legislation?

Professor Norton: No, I agree with those who wrote to *The Times*.

Q343 Chair: You feel that it would hinder innovation and would undermine the privacy of the citizen if this legislation goes through?

Professor Norton: I think these are very complex arguments that have not been properly addressed in that legislation.

Q344 Chair: Mr Coviello, this is almost the last session on e-crime for us. We started this inquiry in November. We have heard about your set-up in Israel with 150 experts trying to protect your clients. Would we be able to find in another part of the world 150 criminals all working together in a similar organisation or in a similar place trying to do exactly the opposite, or is it still tightly knit groups of people all over the world? Has this become now a very organised way of perpetrating crime?

Art Coviello: You would not find them all assembled in one place, but you would find far more than 150 scattered around the world, absolutely. There is no question about that in my mind. To make a guess of whether it is hundreds or thousands I could not speculate, but it is certainly a significant number given the volume and the capabilities and the activity that is going on.

Q345 Chair: I do not know whether you have been to the spy museum in Washington, which I visited last August. As you go in there, the very first video is President Obama with a chilling account of what is happening in cybercrime and how this is the No 1 danger faced in the history of the United States of America, on a par with terrorism. Can you compare what is happening in America to what is happening here? Is it possible for you to tell us is something going on there that is better than what we are doing here or vice versa?

Art Coviello: Unfortunately, no. The internet knows no boundaries, so the attacks can be launched from anywhere to anyone. When I travel to Asia they tell me the attacks are coming from the United States and Europe. When I am in Europe they tell me the attacks are coming from Asia and the United States. So, quite frankly, the attacks are coming from everywhere, and, again, it is incumbent on Government to do exactly what you are doing and I laud this Committee's activity.

One thing I did want to point out: in the charter of your Committee you talk about "increasing the understanding". I contrast that with the word "awareness". There is almost too much awareness. There is not a day that goes by that we do not see some publication, but unless we achieve a high level of understanding we are not going to be able to take the measures necessary to address this problem. Awareness is not it; understanding is, and that is what this Committee is trying to accomplish, and I laud your efforts.

Chair: Mr Coviello, Mr Chantzos and Professor Norton, thank you very much for coming.

Written evidence

Written evidence submitted by the Home Office [EC 00]

Introduction

1. This paper sets out the Government evidence to the Home Affairs Committee inquiry into e-crime. This response refers to “e-crime” as “cyber crime” throughout in order to be consistent with the Government’s Cyber Security Strategy. It has been prepared in consultation with officials from other Government departments including Cabinet Office, Department for Education, Ministry of Justice, Department for Business, Innovation and Skills, Government Communications Headquarters and officers and staff from the Serious Organised Crime Agency (SOCA), the Police Central e-Crime Unit (PCeU), the Child Exploitation and Online Protection (CEOP) Centre and the National Fraud Authority.

2. The Science and Technology Committee previously examined the risks of both malware and cyber crime in the following reports: the third report of the 2010–12 Session entitled *Scientific advice and evidence in emergencies* and the 12th report of that same session entitled *Malware and Cyber Crime.* The Government welcomed both reports as a valuable contribution to its work on cyber crime.

3. The internet has revolutionised our economy, our society and our personal lives. It enables innovative new businesses to start and grow. It allows existing businesses to lower their costs and increase efficiency, and it gives customers the opportunity to demand better, cheaper and more convenient services.

4. However with such benefits and opportunities come threats. The Government’s National Security Strategy, published in 2010, ranked UK cyber security, of which cyber crime is an element, as a tier 1 national security priority. The Government has committed £650m to the transformational National Cyber Security Programme (NCSP) to bolster its cyber defences. Last November, the Government published its Cyber Security Strategy which set out how the UK will support economic prosperity, protect national security and safeguard the public’s way of life by building a more trusted and resilient digital environment.

What is e-crime is understood to be and how does this affect crime recording?

Types of Cyber Crime

5. Cyber crime falls into a number of categories, within the general principle that what is illegal offline is illegal online. The first category encapsulates crimes that can only be committed by using computers and the internet, and that occur where a digital system is the target as well as the means of attack. This includes attacks on computer systems to cause disruption (for example Distributed Denial of Service (DDoS) attacks), and the stealing of data over a network often to enable further crime (for example through the spread of viruses and other malware, or computer and network intrusions (hacking).

6. The second category encapsulates “existing” or traditional crimes that have been transformed in scale or form by the use of the internet, such as fraud or the sharing of indecent images of children. Although these crimes have always existed, the growth of the internet has opened up a new (often global) market, which allows for a degree of anonymity, operation on an industrial scale, and has created new opportunities for organised criminal groups to finance their activities.

7. The final category comprises crimes that use the internet but that are not dependent on it. Here, networks are used for communication, organisation or to try to evade law enforcement. In the same way as the internet is indispensable to legitimate businesses, it can be used to organise more effectively a range of “traditional” crime types such as drug dealing, people smuggling and child exploitation and to conceal them more easily from law enforcement agencies.

8. This is a category of crime that is often neglected when discussing the scope of cyber crime. An increasing number of police investigations of crimes, both serious and volume, now have a cyber crime component, requiring the examination of computers, smartphones and digital CCTV evidence. These may not be recorded as cyber crime, but they do require the police to have access to both the skills and the technology to undertake this type of examination as a matter of routine.

9. The online environment provides opportunities for organised criminals to communicate anonymously, particularly through the use of Internet Relay Chat (IRC) and social media. The sole use of these communication services does not in itself constitute cyber crime, but is a clear example of how technology can assist criminals across a range of activities, including drugs, organised immigration crime and firearms.

10. Knowledge regarding the extent and nature of e-crimes is currently limited, but improving. We have more knowledge regarding some forms of e-crimes than others. It is not currently possible to provide an overall measure of the extent of e-crime. It is also not clear whether e-crimes are decreasing or increasing from the evidence currently available, and whether this varies according to the type of e-crime. However work is underway to address these gaps and gather robust evidence in this area.

Recording

11. There is no such crime as an "e-crime" formally defined in legislation. Police record offences[1] categorised in traditional crime terms, and do not capture offences as a "cyber" or "e-crime". So, whilst a fraud, for example, might be facilitated by use of computers, it would be recorded as a fraud offence, or a denial of service with financial demands may well be recorded as extortion.

12. The computer or other technology used to commit crimes is the method (or modus operandi) by which a crime was committed. The details on methods are not collected centrally. In general, what is illegal offline is illegal online, and UK legislation on fraud or other forms of criminal behaviour applies to both. For example, on-line frauds such as lottery scams, dating scams, boiler room scams all constitute the offence of fraud by false representation, contrary to section 2 of the 2006 Fraud Act. Another example relates to online theft offences, which may be recorded under the Copyright, Designs and Patents Act (1988), Computer Misuse Act (1990) or the Communications Act (2003) depending on what is actually stolen.

13. The Home Office has introduced new crime recording classifications to enable law enforcement agencies to capture specific cyber crime offences as laid out in the Computer Misuse Act (1990), such as computer misuse crime, malware, DDoS attacks and hacking offences.

14. Cyber crime is also captured through victim surveys, such as the British Crime Survey (BCS). The Government is continuing to explore further opportunities to working with the police and other partners to improve the identification of cyber crimes within recorded crimes and crime and victim surveys.

How we are Improving Reporting

15. The Cyber Security Strategy emphasises the importance of increasing the reporting of cyber crimes and there is significant activity under way to address this. The Government has taken steps to expand the role of Action Fraud, which is led by the National Fraud Authority, to become the single reporting point for financially motivated crime. Over the coming months Action Fraud, in partnership with the National Fraud Intelligence Bureau, will press ahead with the roll out of an improved reporting capability to all UK police forces. For the first time the police and the National Fraud Intelligence Bureau will have the capacity and capability to analyse all fraud and cyber crime data from one source. This will provide a much more coordinated and joined up approach to targeting those who attack our citizens and businesses.

What is the extent and the nature of the threats on which e-crime policy is based?

16. In October 2010, the National Security Strategy identified the cyber threat to the UK, which includes cyber crime, as a Tier One threat. £650 million of new funding was allocated to the National Cyber Security Programme (NCSP) which will bolster our cyber capabilities in order to help protect the UK's national security, its citizens and our growing economy in cyber space. At least £63 million of this will go towards enabling the UK to transform our response to cyber crime, in addition to resources ordinarily allocated to law enforcement to tackle crime.

17. There has been some attempt to measure the cost of cyber crime, but it will not be possible to provide a robust estimate until data regarding prevalence and scale of cyber crime has been improved. One widely cited estimate from "*The Cost of Cyber Crime*"[2] produced by Detica in February 2011, approximates the cost to the UK of cyber crime to be up to £27 billion per year, or around 2% of GDP. Whatever the cost, as businesses and Government move more of their operations online, the scope of potential targets will continue to grow.

18. GCHQ is the operational hub for cyber security in the UK and, through its information assurance and intelligence work is the best place in which to concentrate UK expertise in understanding threats and exploiting opportunities in cyber space. GCHQ also hosts the Cyber Security Operations Centre (CSOC), whose role is to provide greater awareness of threats and developments in cyberspace, and ensure that the UK can respond effectively in the event of a major cyber incident. Law enforcement agencies contribute learning from their activities to CSOC. Within the NCSP, a key element of CSOC's role is to act as a central hub, to cultivate a greater holistic awareness of threats, vulnerabilities and developments in cyberspace and to communicate these to NCSP stakeholders and ultimately policy makers. CSOC have produced baseline assessments pertaining to various aspects of the cyber crime landscape and regularly produce topic reports, to which the PCeU, SOCA and GCHQ contribute. The most recent example of this involved contributing learning from their operations in relation to the "Hacktivist" threat.

[1] Police recording of crimes is governed by the National Crime Recording Standard (NCRS) and the Home office Counting Rules (HOCR). These set out the principles under which reports received from victims are recorded. Police recorded crime statistics are based on a notifiable list of offences. The HOCR set out the broad classification groups into which those offences are managed for statistical purposes.

[2] http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

19. The Government is also supporting law enforcement agencies in their work to improve the timely exchange of intelligence with a broad range of industry, academia and other agencies both in the UK and abroad. This intelligence contributes to law enforcement operations and informs threat assessments and subsequent programmes of activity. Intelligence may take various forms, including brigaded victim reports and the latest network vulnerabilities or methodology. For example, the PCeU routinely shares intelligence concerning threats with industry, academic and law enforcement partners, in addition to tactical and strategic learning from their operational and prisoner debriefing activity. The benefits to this approach mean that law enforcement can respond with one timely investigation, rather than dealing with numerous isolated, reports from individual members of the public. Furthermore, once a trusted space within industry is established and a common vulnerability or attack is experienced, then businesses are more likely to report the issue.

20. The cyber crime Threat Reduction Board, established under the Government's organised crime strategy "*Local to Global*" provides an operational context in which law enforcement and intelligence agencies can assess operational and intelligence activity against the Stem, Strengthen and Safeguard themes of the organised crime strategy and provide assurance to Ministers that the cyber crime threat is being effectively tackled. A Cyber Crime Board, chaired by the Parliamentary Under-Secretary for Crime and Security (James Brokenshire MP), has been established to deliver appropriate Ministerial oversight and ensure that policy development is fully informed by the best possible understanding of the threats.

21. *What is the effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and what are the potential impacts of proposed organisational change?*
Are there any gaps in the response to e-crime and, if so, how should they should be addressed?

The Current Law Enforcement Landscape

22. Co-ordination of law enforcement efforts is key to providing a joined up, end-to-end response to cyber crime. Our agencies and law enforcement partners work closely together to make this happen, including the UK Intelligence Agencies, Ministry of Defence (MOD), Centre for the Protection of National Infrastructure (CPNI), Police Central e-Crime Unit (PCeU), Serious Organised Crime Agency (SOCA), HM Revenue & Customs (HMRC), UK Department for Business, Innovation and Skills (BIS), the National Fraud Authority and City of London Police among others.

23. The Government has committed £63 million specifically to tackle cyber crime, which has significantly strengthened the capacity and capability of the PCeU and SOCA. In the first six months of the programme, PCeU operational intervention has resulted in a reduction of impact on the UK independently assessed as £140 million. Last financial year (2011–12) there were 45 arrests for cyber crime with 100% victim satisfaction. Over 21,377 web sites have been taken down from April 2011 to April 2012, resulting from evidence gathered by the PCeU Internet Governance Team.

24. There has been significant progress internationally, specifically cooperation to progress cyber investigations with Ukraine and China, and a cyber Joint Investigation Team (JIT) with Estonia which has been authorised and funded by Europol, and which resulted in substantial prison sentences for an Eastern European organised crime network working in the UK. SOCA has carried out a number of investigations (further details at paragraph 44), and further examples can be found in SOCA's separate submission which sets out its recent successes against cyber crime.

Legislative Capability

25. What is a crime offline is a crime online, and whilst some cyber crime offences such as hacking, phishing, malware or virus attacks are set out in the Computer Misuse Act (1990), many crimes committed online are prosecuted under existing legislation such as the Fraud Act (2006) or the Communications Act (2003).

26. The Government has committed to reviewing the existing legislation relating to cyber crime, to ensure that it is fit for purpose, and remains relevant and effective.

27. In particular, the Government wants the Police and the Courts to have the most effective powers to disrupt, prevent and prosecute those responsible for these crimes. We are therefore reviewing our powers to support law enforcement, including on areas such as gathering and preserving data for use as evidence and information-sharing between sectors and internationally. We have also committed, as part of the Cyber Security Strategy, to encourage Courts in the UK to use existing powers to impose appropriate online sanctions for online offences.

Proposed Organisational Change

28. Subject to the will of Parliament, the National Crime Agency (NCA) will be established by the end of 2013, at the centre of the reformed law enforcement landscape.

29. The National Cyber Crime Unit (NCCU), which will be part of the National Crime Agency, will focus on tackling the first two types of cyber crime, as set out in paragraphs 5 and 6 above. This will allow the NCCU, to focus its resources and skills on the most sophisticated areas of cyber crime, whilst supporting the

NCA and wider law enforcement to take responsibility for tackling cyber-enabled crime. This principle of supporting law enforcement to take responsibility for tackling cyber enabled crime, rather than looking to a specialist cyber unit to lead, will underpin the work of the NCCU. The third definition of cyber crime, that of crimes that are facilitated by the internet, is being tackled through the police who are mainstreaming cyber awareness, capacity and capabilities throughout their service.

30. The creation of the National Cyber Crime Unit (NCCU) is a critical part of the Government's wider National Cyber Security Programme (NCSP). It will bring together the national law enforcement response to cyber crime under one roof. This single capability will work closely with other partners, such as GCHQ, to strengthen the UK's overall resilience and incident response to cyber threats and to ensure individuals and industry can take full advantage of the many opportunities presented by the internet.

31. The National Cyber Crime Unit will deliver a range of benefits to the current law enforcement response to cyber-enabled crime. By bringing together the PCeU and SOCA Cyber, the NCCU will eliminate remit overlaps, delivering efficiencies and spare capacity that can be utilised to bear down harder on organised cyber criminals. Building on the successes of SOCA Cyber and the PCeU, the NCCU will deliver:

- A single, high-profile law enforcement lead dedicated to combating organised cyber criminals;
- A more targeted focus on the most serious incidents of cyber crime, removing the criminals who facilitate cyber-enabled crime further downstream;
- A stronger, more cohesive response to the most serious cyber-enabled crime;
- Dedicated resources to drive a step-change in cyber capabilities across law enforcement, police service and wider partners;
- Stronger partnerships at all levels, including delivery of a single point of contact for rapid response to dynamic threats and closer engagement with industry and academia; and
- Closer joint working with the Security and Intelligence Agencies through improved ICT connectivity and intelligence sharing.

32. Police and Crime Commissioners will be a powerful local representative, able to set the priorities for the police force within their force area, respond to the needs and demands of their communities more effectively, ensure that local and national priorities are suitably funded by setting a budget and the local precept, and hold to account the local Chief Constable for the delivery and performance of the force.

Local Capability

33. In 2008 the National e-Crime Programme conducted a national survey of police capability on cyber. A new project is being developed by PCeU to update this research including staffing numbers, training, equipment and best practice. This will further inform in relation to capability and provide updated information in relation to national response.

34. The publication of the Strategic Policing Requirement will support national co-ordination and collaboration between police forces to respond to serious and cross-border criminality. In order to ensure that local police forces can still access specialist services, the Strategic Policing Requirement seeks to ensure that local policing plans account for cyber capability as well as the contributions that local agencies will provide to the national response.

35. On a national scale, the police response has had limited resources and infrastructure to respond to, exploit, and harness the benefits of the digital environment owing to a fragmented approach to policing cyber crime. The National e-Crime Programme delivered three PCeU hubs to address this situation. The Hubs enhance existing PCeU national operational capability to respond and investigate cyber crime. The regional hubs are based in the North West, East Midlands and Yorkshire & the Humber. The "hubs" were launched in February 2012 and despite their infancy and early stages of development are already contributing to PCeU operations contributing to a fast and dynamic response outside London.

Bringing together Law Enforcement Capabilities

36. Building on the successes of both SOCA Cyber and the PCeU, the establishment of the NCCU will further strengthen the law enforcement response to the most serious cyber crime by addressing a number of gaps that we know exist in law enforcement's response to cyber crime.

37. First and foremost the NCCU will deliver a single, high-profile law enforcement lead dedicated to combating organised cyber criminals. This will provide increased clarity and coherence in the law enforcement response and a more targeted focus on the most serious incidents of cyber crime where the NCCU can add most value.

38. This ambition fits with the overall goal of the NCA to address the sometimes fragmented law enforcement response to serious and organised crime by creating a new Agency with the mandate to task and co-ordinate the UK law enforcement response. The NCCU will form a vital part of the NCA, able to undertake tasking and coordination across the whole of operational law enforcement, ensuring that appropriate action is taken

against criminals at the right level, led by the right agency. The NCCU will also benefit from the NCA's single national intelligence picture of serious and organised crime to inform its operational activity.

39. As part of this, a key principle of the NCCU is to support law enforcement partners to take the lead in tackling cyber and cyber-enabled crime, rather than looking to a specialist cyber unit. We know that mainstream cyber capability across law enforcement needs to be enhanced, and so the NCCU will house dedicated resources to drive a step-change across law enforcement, the police service and wider partners. This will build on the existing work of the PCeU in the National e-Crime Programme, including roll-out of the digital forensic triage tools, supporting the Police Professional Body on developing cyber training, providing a single national centre of expertise to provide guidance to wider law enforcement, as well as ensuring that cyber capability is mainstreamed throughout the NCA itself as a role model for wider law enforcement.

40. The expertise and information needed to combat cyber crime sits largely outside law enforcement including in the Security and Intelligence Agencies (SIAs), industry, international partners and others. The NCCU will draw upon the range of experience and expertise from these partners in order to stay effective against cyber criminals. This will involve closer joint working facilitated by enhanced ICT connectivity and intelligence sharing and maintaining a diverse workforce with experience from a range of sectors. The NCCU will look to utilise NCA Special Constables to bring in the relevant expertise, as well as seconding staff out to industry to strengthen relationships and gain experience. The NCCU will also work with operational partners to ensure that there are clear lines of responsibility when responding to the range of cyber threats, from terrorist cyber attacks to cyber attacks on critical national infrastructure.

41. Given the rapid increase in both the volume of digital data generated by individuals and the range of devices and locations on which it can be found (computers, smartphones, CCTV systems, games consoles, in-vehicle GPS systems, remote (cloud) storage etc.), there is a corresponding increase in the number and type of traditional crimes that now have at least some e-crime component to them. These are generally crimes that would be investigated at a local force level rather than by specialist cyber crime units such as PCeU. One of the key emerging gaps is therefore in the provision at a local level of suitable tools, techniques, skills and common processes to enable the police to routinely investigate these crimes effectively.

Addressing Gaps in the Response

42. In order to improve our local policing response and appropriately direct police resources, law enforcement agencies and the Home Office are working to improve our knowledge around the prevalence and nature of cyber crime, particularly where they relate to volume crimes. This will allow us to effectively train and equip local police officers to tackle these crimes on a day-to-day basis. In this regard, the Home Office Centre for Applied Science and Technology (CAST) is working with policing to evaluate and develop specialist tools and techniques for use both in serious and volume crime investigations, particularly to assist with rapid and automated examination of large volumes of data.

43. Other activities are being considered to improve knowledge on prevalence and nature of cyber crime in relation to volume crime, for example, ensuring appropriate data capture mechanisms are in place and that we are addressing under-awareness and under-reporting of cyber crimes amongst businesses and the general public. More widely, there is consideration around how we address gaps in knowledge regarding "what works" in terms of preventing cyber crime by encouraging the public and businesses to better protect themselves online.

44. There is evidence of a number of successful SOCA, PeCU, CEOP and NFIB disruptive operations in tackling cyber related activities and reporting to agencies such as Action Fraud, NFIB and CEOP has increased. However, wider evaluations of cyber policing structures, initiatives and performance are currently lacking:

- The PCeU have taken forward work to mainstream cyber awareness, capacity and capability throughout their service. The regional hubs of PCeU launched in February 2012 increase operational capacity and capability and awareness of cyber within the regions. Work is ongoing with Skills For Justice to produce a competency framework for PCeU enforcement and intelligence officers. This framework will be available nationally.
- Over the coming year, funding from the National e-Crime Programme is supporting an interim National Hash Set database, which will amalgamate law enforcement databases and apply consistency to grading and processing indecent images of children.
- Virgin Media worked with SOCA to warn customers on its network that they might have been infected with the dangerous SpyEye Trojan variant. This collects personal and banking information and poses a high level threat to infected users. It is comparable in severity to the "Zeus" Trojan which reportedly siphoned over half a million pounds from UK consumers' bank accounts last year. SOCA detected around 1,500 Virgin Media customers' Internet Service Providers (ISPs) infected with the SpyEye Trojan and at risk of identity theft or fraud. Virgin Media wrote to these customers to get help if they were unable to manage the disinfection process themselves.

- SOCA identified and, through its Alerts system, reported several hundred cases of domain name abuse directly to ICANN[3], highlighting continuous failures in the customer validation of domain name registrations by the specific "registrars" directly responsible for the sale of domain names to users. Targeted SOCA Alerts highlighted areas of abuse and registrar practice that disrupted a major online malware distribution group by preventing it from registering and using malicious domain names over a long term period. Collaboration with ICANN to amend the Registrar's Accreditation Agreement (RAA) has assisted law enforcement efforts in crime prevention and detection, and direct reporting to ICANN, highlighting specific criminal use of domain names and methodology, has encouraged due diligence measures to prevent abuse.
- Following a referral from the Internet Watch Foundation, CEOP identified a website that was hosted in Germany, which contained a large number of child abuse material and a section for people to buy and sell children from sexual exploitation. CEOP worked to identify a suspect who was thought to have produced the website and assisted Kent Police in setting up an undercover operation to gather further evidence against the suspect. This was successful and the suspect, Darren Leggett, was arrested. Leggett was found to have committed a number of sexual offences against young children, and was given an indeterminate sentence on 21 June this year, with a minimum term of seven years.
- Action Fraud has reported over 33,000 instances of cyber-enabled fraud or internet crime-related issues, of which 2017 were crimes under the Computer Misuse Act (1990). In addition 19,000 instances of attempted online scams have been reported to the service along with 1,200 reports of virus attacks.

Working with Stakeholders

45. The Government recognises that in tackling cyber crime there is a key opportunity for industry, Government agencies and law enforcement to come together to provide a joint threat picture, to gather intelligence and to provide a joint response.

Building trust and confidence between the private sector and law enforcement authorities is vital to address any gaps in the response the threat of cyber crime. Industry has a vital role to play and also needs to invest in effective information security in order to reduce the threat from cyber crime. We cannot achieve our goals in isolation. The prosperity of the UK, creating a secure UK business environment, a secure UK (critical) national infrastructure is just as important as bringing criminals to justice. The Cyber Security Strategy creates a framework for an alliance that is greater than its constituent parts An excellent example of this cross-sector working is the UK Council for Child Internet Safety (UKCCIS) which brings together government, industry, law enforcement, academia and charities to work in partnership to help keep children and young people safe online.

46. We are now considering how best to build on this successful formula to address the interests of industry and Government in dealing with cyber crime. We are also looking at international partnership models for operational information-sharing, such as the National Cyber-Forensics Training Alliance (NCFTA), based in Pittsburgh, USA. The NCFTA brings together private industry and law enforcement in a neutral, trusted environment to identify, mitigate and prevent cyber crime through joint working and data exchange. We will be looking at this, and other such structures, to inform our work to enhance operational-level partnerships between Government and the private sector on cyber crime.

47. At a tactical level, the PCeU continues to build upon the good work with the existing Virtual Task Force (VTF). The VTF was established in July 2009, incorporates staff from the Police Central e-Crime Unit and has achieved considerable success which has resulted in international recognition of the benefits of this model of public/private sector operational delivery. Member organisations have committed a strategic lead member and tactical representatives.

International Work

48. Cyber crime is an international crime, and the Government has been clear that a major part of our response is to work internationally at Government and at law enforcement levels.

49. The Government has ratified the Budapest Convention on Cybercrime, as the main international agreement in this area, and has taken an active approach to encouraging countries to sign and ratify it. The Government believes that all countries should put in place the appropriate legislation and law enforcement capability to tackle cyber crime, and the ability to support international partners. The Government believes that the Convention offers the only current and comprehensive framework for this.

50. The Government has opted in to the EU Directive on attacks on information systems to ensure that there is common agreement across EU Member States on offences and sentences to allow our law enforcement agencies to together to identify suspects, gather evidence and bring criminals to justice.

[3] Internet Corporation for Assigned Names and Numbers, the body responsible for the administration and allocation of domain names.

51. The Government supports the creation of the EU Cybercrime Centre, and in particular the decision to locate it in Europol, which will build on its existing high-tech crimes capability. The Government expects the Centre to support Member States in working together to tackle cyber crime, and to develop effective best practice in areas such as cross-border cooperation and information sharing.

52. The Government strongly supports the EU Council Conclusions on the creation of a Global Alliance Against Child Sexual Abuse, put forward by the Presidency and the Commission. The Government recognises the need for Member States, third countries, international law enforcement and industry to continue to work together to prevent the spread of child pornography. The Alliance will build on the existing work in this area.

53. The Government strongly supports the work of the Hungarian Government in organising the Budapest Conference on cyber issues that will be held in October. This is a follow up to the London Conference on Cyberspace that was hosted by the Foreign Secretary in November 2011.

What are the options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use?

54. All processing of personal data in the UK, online and offline, must comply with the Data Protection Act 1998 (DPA) and its data protection principles. Importantly, the seventh principle requires that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

55. The expansion of the Internet and the emergence of social media networks has recently led the European Commission to publish proposals for updated data protection legislation. These proposals were published on 25 January 2012 and contain a Regulation (setting out a general EU framework for data protection) and a Directive (covering authorities dealing with criminal offences and penalties). Amongst other things, the proposals seek to provide individuals with strengthened rights to delete their personal data (including a so-called "right to be forgotten"), which could affect the way in which people's information is held by online services, such as social networks.

56. Given the practicalities, costs and potential for confusion of a full-scale "right to be forgotten", the UK Government will push in negotiations for an overhaul of the provisions as drafted. However, the Government is committed to giving individuals the right to delete their personal data, where this is appropriate. The principles of "data minimisation" and "privacy by design", if adopted by organisations in their systems, should help to ensure that people's personal data does not proliferate online and is held securely, minimising the opportunities for those who would seek to use it for criminal purposes.

57. The Information Commissioner, the UK's independent data protection supervisory authority, enforces the DPA's requirements and promotes good practice. As part of the latter role, the Information Commissioner's Office (ICO) has produced guidance for individuals and young people on keeping their personal data safe online, including specific advice on using social networks.

58. There is work under way across Government and industry to improve data protection for customers. BIS and the Home Office are working in partnership with the six major Internet Service Providers (ISPs) in the UK: BT, TalkTalk, Sky, Everything Everywhere, Vodafone, and VirginMedia, to explore what more could be done or done differently to better protect businesses and consumers from online threats such as malware and botnets. This covers the basic security packages that ISPs are offering to their customers, as well as raising awareness amongst customers about the importance of behaving securely online.

59. Further work is under way with Government, industry and law enforcement through the Forum for Innovation in Crime Prevention. This is a strategic expert advisory group drawn from science, business and industry, law enforcement agencies and Government that identifies major opportunities for preventing and disrupting crime through innovative design, technology and behavioural change and proposes solutions that incentivise business engagement.

60. Our law enforcement agencies work with their counterparts overseas to carry out work such as restricting criminal access to the Internet. This is achieved through work with organisations such as the Internet Corporation for Assigned Names and Numbers.

How effective are current initiatives to promote awareness of using the internet safely and what are the implications of peoples' online behaviours for related public policy?

61. Prevention is key, and we are working to raise awareness and to educate and empower people and firms to protect themselves online. GCHQ estimates that 80% or more of currently successful attacks could be defeated by simple best practice, such as updating anti-virus software regularly. The Government works in close partnership with industry on cyber security, recognising that this is crucial to protecting individuals and their data.

62. Organisations can be attractive targets for cyber criminals, who may seek to exploit security vulnerabilities in order to access intellectual property or other commercially sensitive information. In the Cyber

Security Strategy, the Government committed to improving both the information sharing and risk management between businesses, law enforcement and business service providers.

63. The Government supports Get Safe Online, which is a joint public and private sector campaign which provides up to date, accurate and authoritative advice to online consumers on how to protect themselves, their families and their businesses online. We have increased funding for Get Safe Online to £395,000 this year to improve the website and enable it to reach out to more people across the UK. The campaign is working in partnership with various police forces, as well as their private sector partners to provide advice on cyber security that is accessible to everyone.

64. Action Fraud has a key role to play in terms of encouraging and enabling behaviour change in relation to preventing citizens and businesses from becoming victims of crime in this area. An excellent start has been made in this arena with the successful delivery of the "Devil's in Your Detail" campaign which was a joint initiative between the NFA and private sector organisations from the banking and telecoms industries. This campaign was video-driven and aimed to encourage people to treat their personal information as a valuable commodity. The campaign reached over four million people. Subsequent analysis of 4,000 people who watched the videos resulted in over 60% stating that they would take more steps to protect themselves from fraud.

August 2012

Written evidence submitted by the Serious Organised Crime Agency [EC 01]

Introduction

1. This submission sets out the Serious Organised Crime Agency's (SOCA) written evidence to the Home Affairs Select Committee's inquiry into e-crime. In the terms of this response we will refer to e-crime as cyber crime throughout the submission.

2. The submission outlines the current level of knowledge within the organisation on cyber crime. This submission has been written in coordination with the Home Office, and should be considered supplementary to its submission.

What e-crime is understood to be and how this affects crime recording

3. SOCA works with its partners, under the Home Office's Organised Crime Strategy ("Local to Global"), to address the threat of organised cyber crime. Under the Strategy, the multi-agency Cyber Threat Reduction Board[4] (TRB), chaired by SOCA, adopted the following definition of cyber crime in November 2011:

- "pure" online crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to enable further crime);
- "existing" crimes that have been transformed in scale or form by their use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale; and
- use of the internet to facilitate drug dealing, people smuggling and many other "traditional" types of crime.

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

4. Organised crime is increasingly globalised and IT-enabled, a trend inevitably accelerating with society's dependence on the internet. Organised criminals operate their own self-regulated market for cyber crime goods and services, including stolen data, malicious software, technical infrastructure and money laundering: and they operate on an industrial scale. As more data is acquired, stored and shared and ever increasing use is made of mobile devices, so the risk increases. SOCA contributed to the development of the Government's Cyber Security Strategy which was published in November 2011. The Strategy references research suggesting that the costs to the UK of cyber crime could be in the order of £27 billion per year.[5]

5. SOCA, along with other departments and agencies, has also played a part in contributing to activity led by the Department of Business, Innovation and Skills (BIS), helping to raise awareness at a senior level within private sector organisations of the threat posed by on-line crime to business performance, shareholder value, reputation, intellectual property and the security of information systems.

[4] Threat Reduction Boards were established under the Government's Organised Crime Strategy to provide focus for law enforcement partners including HMRC, SOCA and UKBA. Each board is chaired by a senior operational partner, responsible for assessing operational and intelligence activity against the three themes set out in the Organised Crime Strategy (stem, strengthen, safeguard). The activities of the boards are subject to scrutiny by the senior officials group and Ministerial structure

[5] "The Cost of Cyber Crime", Detica—14 February 2011

The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

6. Key activity aligned to the Organised Crime Strategy in respect of cyber crime includes:

— improving the understanding of, and intelligence about, cyber crime in order to identify changes to drive the response;

— ensuring that the operational response to cyber crime is being coordinated effectively and is reducing the risk to the UK of cyber crime; and

— providing assurance that identified organised crime groups are subject to an appropriate level of operational response and that the maximum impact against the threat area is being achieved, improving our understanding of the threat that impacts on the UK.

7. SOCA responded to the Government's National Cyber Security Programme by expanding its current cyber capability, including the posting of dedicated Cyber Liaison Officers in key locations overseas.

8. Recent successes achieved against cyber crime include:

— a SOCA led global day of action took place on the 25 April 2012 to tackle Automated Vending Cart (AVC)[6] websites selling compromised financial data. Two UK arrests were made and SOCA intelligence assisted the US in seizing data for 26 AVCs and 36 domains. In addition, as a direct result of eight alerts issued, a further 44 AVCs have been taken down—resulting in significant disruption.

— in 2011–12 SOCA and its partners seized over 1,200,000 items of compromised card data from cybercriminals and passed these details to industry via the Alerts system.

— as a result of SOCA operational activity two men who provided a range of services to credit card fraudsters were sentenced to almost five years imprisonment after facilitating fraud valued at more than £26 million. Both pleaded guilty to a range of fraud, money laundering and computer misuse offences, and were sentenced at Bristol Crown Court to three years and 21 months respectively. Forensic analysis revealed payment card details of more than 340,000 individuals. The estimated losses are a conservative figure and the actual loss is likely to be considerably more. In addition, the information brokered would also have been sufficient to enable fake bank accounts to be set up, which could be used to commit further fraud, such as cheque or identity fraud.

9. SOCA has been involved in dealing with cyber crime on an international level as well. Cyber crime investigations almost inevitably have an international element, with criminals, data and infrastructure typically based across multiple jurisdictions. SOCA has therefore developed close working relationships with many foreign partners, which enables intelligence sharing, evidence gathering—support with the preservation of data in particular—and operational engagement. Recent examples include joint working on the selling of compromised financial data online. A coalition of overseas partners worked together to make arrests and take down websites, multiplying the effectiveness of UK law enforcement activity. Tackling cyber crime internationally will also require new ways of working. The UK is working closely with Interpol, Europol and United States partners to establish more innovative approaches to tackling cyber crime.

10. Mainstreaming of cyber capabilities is underway within SOCA, and will harness the potential of every investigator to use cyber crime tools, not solely those from dedicated cyber units. All officers will receive training on cyber crime, internet security, open source capabilities and online investigation techniques, following the completion of a comprehensive training needs analysis. SOCA operational teams have embedded officers specialising in digital forensics and open source research, making these techniques more readily available at every stage of an investigation. In addition, officers with a dedicated cyber remit have also been placed within other key business areas enabling cyber mainstreaming to grow from within departments.

11. Going forward, the National Crime Agency (NCA) presents the UK with the opportunity to improve its national law enforcement response to crime perpetrated in cyber space or enabled by the internet, through the establishment of a National Cyber Crime Unit (NCCU). The NCCU will act as a centre of expertise for tackling cyber crime. The NCA will have the specialist operational capabilities and the latest technology to ensure that its intelligence gathering and analytical capabilities match the threat posed by cyber criminals. It will bring together the digital investigation capabilities of SOCA and the MPS Police Central e-crime Unit (PCeU) to provide an enhanced response to the cyber crime threat.

Whether there are any gaps in the response to e-crime and, if so how they should be addressed

12. There are a number of factors that can hinder law enforcement in the response to cyber crime. For example, the majority of cyber criminals are not within UK jurisdiction, and international barriers inhibit their identification and prosecution. Differing domestic legislation is also an issue, for example in some countries cyber crime is not recognised in domestic legislation.

[6] Automated Vending Cart (AVC) is a term coined by SOCA (and now adopted internationally) to describe click and buy e-commerce websites that automate the sale of compromised personal financial data

13. In response SOCA has worked closely with the Foreign and Commonwealth Office and other government departments to encourage the implementation of legislation and recognition of cyber crime in key countries. For example the Commonwealth Initiative has agreed to target priority countries for assistance.[7] SOCA Cyber Liaison Officers overseas will work to ensure that cyber crime is also identified as a priority and enhance overall international relations.

14. The UK is also working with global partners to encourage wider adoption of the Budapest Convention on cyber crime, putting in place compatible frameworks of law that enable effective cross-border law enforcement and deny safe havens to cyber criminals.[8]

15. Beyond those law enforcement agencies with a specialist role there is also a general lack of awareness of cyber crime, which hinders the ability to investigate and target both "pure" cyber crime and "digitally enabled crime". It is essential that the message is conveyed across the whole law enforcement community that cyber crime is a priority. The establishment of the NCCU in the NCA, bringing together SOCA and other cyber law enforcement units, will help to further improve the UK's response.

Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use. The effectiveness of current initiatives to promote awareness of using the internet safety and the implications of peoples' online behaviours for related public policy

16. The Government's Organised Crime Strategy identified "Safeguarding" as one of the key themes for tackling organised crime by reducing the vulnerability of communities, business and the state to become victims of crime. In line with this theme SOCA supports raising awareness of cyber crime to prevent consumers becoming victim to cyber criminals. For example, Get Safe Online (GSOL) is one a number of initiatives between the Government, SOCA, and the private sector. This highlighted the increased use of smart phone malware during "Get Safe Online Week" in November 2011. Criminals use online application stores to entice smart phone users to download rogue applications. The malware is often disguised as "free levels" to popular and legitimate games, or even as security tools. Users are often unaware that fraudsters have control of their phone (and access to personal and payment data) until they receive their monthly bills or otherwise find themselves victims of identity crime. GSOL has produced a free download, The Rough Guide to Online Safety, in order to reduce the threat.

11 July 2012

Supplementary written evidence submitted by the Serious Organised Crime Agency [EC 01a]

During my appearance before the Committee on the 11 December 2012 to give evidence to the e-Crime inquiry, I promised to write listing the EU Justice and Home Affairs (JHA) measures that SOCA utilises in regards to cyber crime investigations.

There is extensive law enforcement collaboration at an operational level between SOCA and partners across Europe, which supports and informs EU policy. This joint activity takes place through a number of JHA measures. I set out details of these, with a particular emphasis on cyber crime below.

- With the support of other UK law enforcement agencies, SOCA has established a multi-agency UK Liaison Bureau at Europol which, via a network of other national liaison bureaux and contact points, coordinates international operational engagement with other Member States and third countries/organisations which have cooperation agreements with Europol. The UK (SOCA) participates in Europol's Focal Points Cyborg, Twins and Terminal, working with other partners to address the threat of cyber crime through operational cooperation and sharing intelligence, utilising Europol's expert analytical capability as the EU's information hub to identify opportunities for further cooperation.
- On 11 January 2013 the EU Cyber Crime Centre based within Europol opened. This centre will support Member States and EU institutions in coordinating operations and investigations with international partners in line with Europol's wider mandate; and, will provide an expert analytical capability to partners. The Centre will improve evaluation and monitoring of existing preventive and investigative measures, support the development of training and awareness-raising for law enforcement and judiciary, establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs).

[7] The Commonwealth Initiative is a new multi-stakeholder approach to developing a safe cyberspace internationally, drawing together the combined mandates of existing organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the United Nations Office on Drugs and Crime (UNODC), Council of Europe, International Telecommunications Union (ITU) and Commonwealth Secretariat to develop and implement coherent, holistic cyber capacity building programmes for developing Commonwealth states. It is co-funded by the UK Government (Department of Culture Media and Sport). SOCA chairs the Executive Board

[8] The Budapest Convention on Cyber Crime is the first international treaty on crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

- SOCA also participates in a European Multidisclinary Platform against Criminal Threats (EMPACT) project on cybercrime, which is led by Romania. This is one of eight EMPACT projects overseen by the EU Standing Committee on Operational Cooperation on Internal Security (COSI) set up to streamline and help coordinate operational cooperation on priority threats to the EU, as part of the EU Policy Cycle on serious and organised international crime. Europol plays a supportive role to this work, through its Focal Points, hosting project meetings and assisting in coordinating operational activity associated with the project.
- SOCA also partakes in the use of Joint Investigation Teams (JITs) to support international operational engagement. The use of JITs provides a mechanism for Member States to cooperate operationally, establishing a clear agreement between participating countries setting out terms of engagement for cooperation and information sharing in accordance with Member States' national legislation. Both Europol and Eurojust provide support to JITs; Europol in providing analytical support and Eurojust in providing judicial expertise, legal assistance and funding.

In addition to the above measures SOCA also regularly utilises the following JHA measures:

- European Arrest Warrant.
- Schengen Article 40.
- Financial Intelligence Unit (FIU) Cooperation.
- Asset Recovery Offices (ARO).

Andy Archibald
Deputy Director
Serious Organised Crime Agency

Written evidence submitted by the British Retail Consortium [EC 02]

1. *Introduction*

1.1 The British Retail Consortium (BRC) is the lead trade association for the retail sector representing the whole range of retailers, from small independent stores through to the large multiples and department stores, selling a wide selection of products through centre of town, out of town, rural and online stores.

2. *Summary*

2.1 Retail is at the heart of local communities, employing close to three million people across the country and providing important local goods and services to consumers. The sector is an essential contributor to economic growth and to the regeneration of areas affected by crime and disorder.

2.2 Online retailing is a significant element of the future strategy for many businesses and increasingly important to the economy. The value of UK internet retailing in 2011 was £25 billion (up from £21 billion in 2010). Internet sales growth averaged 15% in 2011 and the sector represented 10% of total retail spending over the 2010–11 period. The growth of e-commerce and corresponding opportunities for increasing fraudulent behaviour should not be underestimated. Retailers need to be sure that as they seek to expand their businesses via e-commerce the customers they attract will be well protected. Retailers invest significant resources in protecting their customers. But, too often, the current law enforcement response to e-crime and fraud is inadequate. The BRC is calling for a dedicated national unit tasked to investigate and respond to the increasing levels of e-crime.

2.3 Engagement between the private sector and law enforcement agencies should be focused on finding the most effective way to achieve a better response to e-crime and fraud. The focus must be on finding ways in which the public and private sectors can work more effectively together to reduce the level of offending and to raise consumer confidence.

3. *What e-crime is understood to be*

3.1 The BRC uses the following ACPO definition of e-crime:

3.2 *The use of networked computers or internet technology to commit or facilitate the commission of crime.*

4. *The effectiveness of current law enforcement and the potential impacts of proposed organisational change*

4.1 Retailers are concerned that the law enforcement community has failed to keep pace with the rapidly expanding threat of e-crime. This situation may be exacerbated in the future by diminishing police resources and the introduction of locally elected police commissioners who may, in some cases consider business crime a low priority.

4.2 A number of BRC members have reported dissatisfaction with the level and quality of communications they receive from the police regarding e-crime. Retailers want far more clarity about what they can expect in terms of support and engagement throughout the process of prevention, detection and punishment of e-crime and fraud.

4.3 Retailers are generally dissatisfied with current police responses to e-crime and often do not report incidents. The reason for this is that e-crime is not considered to be a priority for many police forces. There are also concerns that national units such as the National Fraud Intelligence Bureau of Police Central e-Crime Unit (PCeU) do not have the resources or capacity to carry out further investigations.

4.4 Currently, there is no mechanism for retailers to report offences directly to Government/the law enforcement community via a centralised model for reporting. BRC members believe that this would be a valuable innovation which would permit more effective analysis of combined data from all sectors. It would also ensure greater awareness of the threat of e-crime to the UK and better inform the public, private and SME sector about potential threats to their businesses.

5. *Gaps in the response to e-crime and how they should be addressed*

5.1 The central concern of BRC members relates to the case acceptance criteria for each of the national agencies who deal with e-crime and fraud. Too often, retailers find themselves preparing detailed reports with the expectation that the relevant agency will accept the case. However, because of the opaque and diverse range of case acceptance criteria, retailers frequently find their case falls just short of the requirements for acceptance. When offences do not reach the acceptance criteria they need to be reported locally. Retailers therefore need clarity around where, in the first instance, offences should be reported and, if they must be reported locally, then it is vital that local operational capacity is available to progress an investigation adequately.

6. *Options for addressing key emerging issues*

6.1 The BRC has identified two distinct areas where challenges are likely to arise in the future. These are the increase in the use of mobile technology and the introduction of locally elected Police and Crime Commissioners.

6.2 The shift towards m-commerce will undoubtedly bring a number of challenges for the retail sector. The balance between providing flexibility for consumers versus protecting consumers and brands will become increasingly complex.

6.3 Some industry observers predict that mobile payments are likely to be an important trend for the future and fraudsters will certainly be looking to exploit this new channel. However, until adoption increases it is too early to tell exactly where the risk lies for merchants. What is clear, however, is that retailers will have to become increasingly aware of the end-to-end process involved in m-commerce and understand exactly where the risks and liability lie for any fraud that is carried out.

6.4 However, developments in electronic crime are fast paced and highly unpredictable. BRC members would like to see the Government and law enforcement community issuing alerts on key and emerging threats to UK retail businesses and working with these businesses to ensure that the threats against them are clearly understood.

6.5 The British Retail Consortium is supportive of the introduction of elected PCCs. Retailers across the UK are keen to work with the police to build and support safer communities. We believe it is important that newly elected PCCs are supported in reconciling demands from the community and the needs of business when setting local policing priorities. It is also vitally important that candidates have opportunities to engage with a wide range of stakeholders before the elections and that, if necessary, Government should facilitate this.

6.6 It is also vital that new PCCs are encouraged to share best practice to ensure that crime is tackled consistently across England and Wales. This is especially true for retailers who operate national businesses and expect a standard response from the authorities no matter where a crime takes place. A consistent approach is vital when tackling e-crime and fraud.

7. *The effectiveness of current initiatives to promote awareness of using the internet safely*

7.1 Retailers invest heavily in anti-fraud systems and are continually seeking ways to safeguard themselves and their customers. However, more needs to be done to encourage consumers to keep their details safe. As e-commerce grows, the burden of educating customers must be spread further than the retail sector. There is a real role for the Government and the third sector to provide such support. BRC members would welcome a Government campaign aimed at helping consumers stay safe online.

7.2 Emphasis also needs to be placed on the public keeping their details safe offline as well—information collected in the real world is often used as the basis upon which virtual crimes are perpetrated. Though these precautions alone will not eliminate e-crime and fraud, they are part of a package of steps that can be taken to reduce the risk of crime.

8. *BRC recommendations*

8.1 In in our 2011 report *The Futures of E-crime*, the BRC made six key recommendations around how to make the future of online sales more secure:

8.1.1 Improve Law Enforcement Communication

8.1.1.1 Communication between law enforcement agencies and retailers should be improved so that each is clear about the evidence that is needed to support a successful investigation. Frequently law enforcement agencies waste time and resources by unnecessarily conducting investigative work which has already been undertaken by the retailer.

8.1.2 Clearly Define Law Enforcement Responsibilities

8.1.2.1 There needs to be more comprehensive information about which law enforcement agencies have responsibility for e-crime and online fraud, and the extent of those responsibilities. Such information should identify overlaps and intelligence gaps. There should also be greater transparency about the case acceptance criteria for each of these agencies.

8.1.3 Make Effective use of Intelligence

8.1.3.1 The National Fraud Intelligence Bureau should work with third party screening companies to enable more effective use of intelligence. There is a wealth of intelligence held by third party screening companies which could prevent offences occurring by enabling action before an offence is committed. This would reduce the number of victims and help provide reassurance to the public that they are being fully protected.

8.1.4 Undertake a National Threat Assessment

8.1.4.1 There should be a National Threat Assessment on Online Shopping. This will help to identify the extent of the need for an economic crime capability as part of the new National Crime Agency.

8.1.5 Communicate with Banks/Card Issuers

8.1.5.1 There needs to be better communication and information exchanged between the bank and card issuers, and retailers to facilitate greater detection and prevention of e-crime and fraud.

8.1.6 Identify Effective Practice

8.1.6.1 Good practice guidance should be developed to enable retailers to reduce incidents of internal fraud and to increase the understanding of how to best protect consumers. Police forces should be encouraged to share best practice on how to engage with retailers and each other on detection and prevention of e-crime and fraud.

August 2012

Written evidence submitted by Engineering the Future [EC 05]

This is an *Engineering the Future r*esponse to the Home Affairs Select Committee call for evidence on E-Crime.

This response has been developed by:

— BCS, The Chartered Institute for IT.

— The Institution of Engineering and Technology.

The response is supported by:

— The Engineering Council.

— The Institution of Mechanical Engineers.

— The Royal Academy of Engineering.

Please note that a glossary of terms that are used in this response is provided at the end of the submission.

1. *What e-crime is understood to be and how this affects crime recording*

"E-crime" (and its near-synonym "cyber-crime") is an ambiguous term that is used to mean, variously, crimes whose nature intrinsically requires the involvement of one or more computers. These offences fall within the remit of The Computer Misuse Act or what might be termed "traditional" crimes, such as fraud or extortion, where the use of a computer is a subsidiary element. Crimes such as "phishing", where an email is used to obtain private information for fraudulent purposes, possibly in concert with a fraudulent website, are recent variants on a technique known in the security community as "social engineering" and among journalists as "blagging".

For this reason, any reported statistics that purport to state the extent of, growth in, or damage caused by cyber crime or e-crime, should be regarded with considerable caution unless they are accompanied by full definitions of these terms, a breakdown of the incidents that fall into each sub-category and full details of how any losses have been calculated. It would be absurd, for example, to count every illegally downloaded music track as a lost sale at the retail price, just as it would be absurd to assume that everyone who buys a fake Rolex watch at a car boot sale was, in fact, intending to buy the real thing.

It is noticeable that the highest estimates of the prevalence of cyber crime or cyber attacks come from organisations whose business depends on the sales of technical countermeasures or whose budgets could be seen to depend on the degree of alarm about cyber security within government. So far as we are aware, there are no independently verified statistics about the extent of any individual categories of cyber crime.

It is likely that a great deal of e-crime goes unreported and unrecorded. Most internet users will receive several phishing emails, malicious attachments or attempted money-laundering or advance-fee-fraud approaches each week. In practice, most of these will be deleted. While there is a facility for recipients to forward such email to phishing@cityoflondon.police.uk with all the headers intact, it is unclear whether they are recorded or are followed up.

While the police are the natural first line responders for any crime, few of the UK's 52 geographical police forces have the expertise and the resources to deal with large scale e-crime, especially on a national or international scale. While there are specialist units, the UK does not have a single authority for the reporting and investigation of e-crime. The present system appears to lack the coordination and process to reassure the citizen and deal with an industrial scale threat. Victims and suspected victims of e-crime would benefit from a greater awareness, more transparency and a single point of contact when seeking advice and incident reporting.

2. *The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers*

The Cabinet Office has stated that government and the citizen are affected by rising levels of e-crime, at an estimated cost of £2.2 billion and £3.1 billion respectively. However it acknowledges that business bears the lion's share of the cost of e-crime, at a total estimated cost of £21 billion.[9] These figures should be treated with caution for the reasons given earlier. It is clear, however that e-crime is a significant threat to UK citizens and businesses.

The rapid growth of eCommerce increases our dependency on the availability and integrity of the internet and our computer and communications infrastructure. While the extent of that dependency is easy to understand in terms of the potential impact of the denial or corruption of those services, it is more difficult to comprehend the true extent and nature of the threat. The source of the threat is extensive, ranging from the substantial resources of a nation state to the ingenuity of an inspired individual or the copycat behaviour of "script kiddies" (see glossary of terms, page 6). The nature of the threat is variable depending on the business and technology employed. However, in the modern industrial-size processing environments on which our economy depends, the integrity and availability of information will remain our principal vulnerability and the focus of any attack, while the vulnerabilities in systems controlling industrial plant and national infrastructure should not be overlooked.

Some threats have been researched, clearly defined and are understood by policy makers: such as online child exploitation covered by Child Exploitation and Online Protection Centre (CEOP) and understanding of online phishing, identity theft and crimes involving financial fraud by the Serious Organised Crime Agency (SOCA). However other areas like bullying online, defamation, invasion of privacy, particularly where social media are employed, are not so well defined or understood by policymakers.

The UK is experiencing a period of rapid social, economic, technical and political change which has engendered a more challenging and permissive environment. New technology enables a raft of traditional non-violent crimes to be committed in new ways, across borders and at scale previously unimagined. Policy makers must remain vigilant and maintain a far greater awareness of the potential and the vulnerability of our information society to malicious attack.

3. *The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change*

Law enforcement in the UK struggles to address the magnitude of the task of combating e-crime. While there are some notable successes in combating serious online crime, anti-terrorism and espionage, the vast bulk of e-crime inevitably goes undetected or unreported and therefore unresolved. Policing is nearly non-existent at the more mundane levels that most citizens experience e-crimes. This is very serious since it creates an impression that the police do not care about e-crime as it affects the ordinary citizen, particularly where the local response is close to non-existent or patchy at best. E-crime is now much more frequent than physical crime but is largely unrecorded and unresolved.

There is growing action to increase the percentage of police officers who have been trained to handle the burgeoning amount of digital evidence that is relevant to solving and successfully prosecuting all kinds of crime and this will increase the potential resources that could be used to address the more serious forms of e-crime. Resources will always be limited and the potential task faced by the police is huge. A single seizure following a referral by CEOP may contain hundreds of hard disks containing hundreds or thousands of

[9] www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

gigabytes of data, dozens of mobile phones and other digital devices. These will need to be properly recorded, managed and controlled to preserve the evidence chain, and forensically examined as a matter of urgency as a child's life may be at risk. Yet each phone examined and each email chain may lead to one or more addresses across the country that must be searched and where similar scale seizures may be required. Resources are soon stretched beyond breaking point.

Recent legislation has promised much but delivered little to aid the combating of e-crime. The Digital Economy Act 2012 has been widely perceived as supporting intellectual property interests and placing the onus of policing on the ISP, while potentially stifling creativity and offering little in the way of protection to the citizen with few barriers to those who wish to avoid the additional restrictions. In effect, the planned legislation has been designed to address the perceived terrorist and organised conventional crime threat, rather than addressing the wider e-crime threat which in an international context may not be within its powers. The election of Police and Crime Commissioners may affect the priority that local Chief Constables give to e-crime but will not increase the available resources. The Strategic Policing power that the Director General of the new National Crime Agency (NCA) will have is a further factor that will influence prioritisation by Chief Constables. The cyber resources of the NCA will be limited and will probably be directed against the highest priority targets.

While the devolved administrations of Scotland[10] and Wales[11] have introduced schemes to better coordinate the fight against e-crime little progress has been made on a UK scale. Proposed organisational change appears to offer little in the short term to combat the rapid growth in e-crime and provide greater clarity and reassurance to the citizen.

4. *Whether there are any gaps in the response to e-crime and, if so, how they should be addressed*

The UK response to e-crime presently lacks the clarity and co-ordination seen elsewhere in the world.[12] There needs to be greater clarity about the types of e-crime, with a clear definition and understanding of what is criminal, what is civil and where responsibility lies between business and law enforcement. There needs to be a simple well-coordinated process for reporting e-crime with clear lines of responsibility for recording, investigating and where necessary apprehending and prosecuting offenders. We need to move away from any presumption that the banks' technology is secure and that customers who report fraudulent activity on their accounts are at fault or lying—there have been too many examples of weaknesses in banks' security for it to be reasonable for the burden of proof to lie with the customer.

There are major problems in investigating crimes and pursuing criminals where the offence originates overseas. The UK does not have the same power to require foreign telecommunication service providers to provide communications and user data that can be required from UK-based companies. Attempts to negotiate bilateral agreements could easily founder because of understandable reluctance to open UK companies' and citizens' private data to scrutiny by agencies in countries that may have national interests that are not wholly aligned with the UK's. Our growing dependency on technology and the magnitude of the threat demands a balance of legislative framework and administrative structures that protect the citizen while supporting e-business and innovation; promoting the UK as a safe well regulated environment in which business can thrive. To achieve this will require a more collaborative approach between the public and private sector in addressing the threat and the acquisition and development of new capabilities and skills by our regulators and law enforcement professionals.

5. *Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use*

The massive and growing volumes of personal data held by social networking sites already expose individual users to significant risk. This data can be employed for a wide range of criminal purposes including identity theft, extortion, stalking, and defamation. Our society has embraced a more open and transparent attitude to free expression and personal information. While embracing this culture, individuals need to be aware of the risks they expose themselves to and the level of personal accountability and liability they must accept. They also need to understand the precautions they need to take to minimise their personal exposure to malicious attack. At the same time, all large databases of personal information need to be designed and managed in a way appropriate to the risk to citizens if the data is misused. In general, this should mean that such databases conform to GCHQ guidance for databases handling secret data and, where they do not, the data controller should carry liability for any misuse of the data.

In attempting to address this issue any legislative framework must be perceived as fair, setting the right balance between protecting an individual's right to privacy and protecting society from irresponsible behaviour. The frequently employed analogy is that of the Highway Code, where a set of laws and best practices have been applied for the common good to protect the users of our roads and the individual must operate within those rules or face legal or commercial penalties. Perhaps we need to capitalise on aspects of this analogy in mounting a national education campaign to improve awareness of our vulnerability to e-crime and correctly assign accountability for protecting our personal data.

[10] www.ecrimescotland.org.uk

[11] www.ecrimewales.com

[12] www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/default_en.asp

Nevertheless, it is essential to recognise the software vulnerabilities that expose computer users to risk, through the propagation of viruses and worms. The capability of seemingly benign attachments, such as pdf files or jpeg pictures to execute malicious code or website attacks such as SQL injection, all result from wholly avoidable mistakes by the developers of the faulty software. It is misguided and ineffective to try to change the natural way in which millions of computer users use their computers without creating sufficient incentive for software manufacturers to create products that do not expose their customers to such serious risks. We would like to see a timetable announced for introducing a Europe-wide measure of liability on manufacturers and importers of faulty software for the damage that these avoidable defects cause. This would build on the precedent set by the Consumer Protection Directive and similar UK legislation and should similarly allow a state-of-the-art defence.

6. *The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples' online behaviours for related public policy*

Current national initiatives appear to have been largely ineffective. The "Get safe online"[13] joint initiative between the government, law enforcement and leading businesses provides free, independent, user-friendly advice to users that allows them to use the internet confidently, safely and securely. While an excellent concept which was well implemented, it has not been widely promoted and there is little evidence that it has achieved significant engagement with the citizen or commerce. In any case, the guidance cannot address the real sources of vulnerability, as explained above.

BCS has produced the "Personal Data Guardianship Code" and "Top Tips for Security" to better protect personal data and improve computer and internet security. Whilst these have been deployed by a growing number of public and private sector organisations, the impact on the bulk of online users has been minimal.

To enable any new initiatives to succeed requires a co-ordinated, comprehensive, continuing education and change programme aimed at changing peoples' online behaviours by increasing awareness and creating a safety conscious online society although, as we said earlier, the main source of risk is not, as widely claimed, unsafe behaviour by computer users but, rather, the design flaws and programming errors that make normal, reasonable behaviour unsafe.

Glossary of Terms and Acronyms

pdf—Portable Document Format—A standard for storing documents electronically in a form that is readable on most computer platforms using freely available reader software. File names often end with a "pdf" file extension.

jpeg—Joint Photographic Expert Group—A file format commonly used to electronically store graphical/ photographic images. File names often end with a "jpg" file extension.

SQL injection—Structured Query Language. A common database language used to extract or display information held within a database. The injection element refers to a process whereby SQL commands can be inserted within user input strings, such as usernames, addresses or passwords, to exploit system weaknesses that in turn may allow access to the database or operating system in a way that effectively bypasses system security checks and safeguards.

Script kiddies—Usually fall into the category of younger or immature users who unfortunately can often be dangerous exploiters of security vulnerabilities in communications systems such as the Internet or the attached computer based systems. A typical script kiddy uses existing and frequently well known, easy-to-find techniques and programs or scripts to search for and exploit these vulnerabilities. These are often carried out randomly with little regard or perhaps even understanding of the potentially harmful consequences of such actions.

August 2012

Written evidence submitted by the Foundation for Information Policy Research [EC 06]

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

Last year, the Cabinet Office put its imprimatur on a marketing brochure from Detica claiming that the UK was losing £27 billion a year to cyber-crime. This was greeted with widespread ridicule, whereupon Sir Mark Welland, then Chief Scientific Advisor at the Ministry of Defence, asked us whether we could come up with more defensible numbers. The result was "Measuring the Cost of Cybercrime", a major study of what's known and what's not known about cyber-crime, in the UK and internationally. This was published in June at the Workshop on the Economics of Information Security, the leading peer-reviewed academic conference in the

[13] www.getsafeonline.org/

field. The authors included two members of FIPR's advisory council (Ross Anderson and Richard Clayton) plus industry experts and academics from the UK, the USA, Germany and the Netherlands.

We urge the Committee to read our report, which we include here by reference[14]. Its main points are summarised below.

1. The Committee first wants to know "what e-crime is understood to be and how this affects crime recording". The EU issued a Communication in 2007 where the definition extended from traditional forms of crime such as fraud and forgery committed over electronic networks, to crimes unique to electronic networks such as service denial attacks. Our report teased this out into three categories. The first, the traditional frauds now conducted electronically, includes tax fraud and welfare fraud as its biggest components by value. The actual crimes here are mostly unchanged from a generation ago, having to do with misrepresentation of circumstances rather than any technical wizardry. The second, which we called "transitional cybercrime", consists of crimes such as card fraud which existed already but where the modus operandi has changed almost completely. The third, the "pure" cyber-crimes which did not exist before the Internet, range from stranded-traveller and fake escrow scams to extortion via fake antivirus software.
2. The UK government takes a different view. VAT fraud is not seen as cyber-crime despite the fact that all VAT returns are now filed electronically. Most seriously, it has been policy since 2005 to tell fraud victims to report the fraud to their banks first. This had the advantage, from the viewpoint of the Home Office, of making fraud almost disappear as a recorded offence. Yet according to the British Crime Survey UK households are more than twice as likely to be victims of fraud as of "traditional" acquisitive crimes such as burglary and car theft; and according to Eurostat's 2010 survey, the UK ranks second behind Latvia for fraudulent payment card use and for losses caused by phishing/pharming.
3. The Committee's second question is "the extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers". In our experience, policymakers have a very poor understanding of cyber-crime; it is truly disturbing that the Cabinet Office was willing to co-brand the Detica brochure. Policy appears to be driven by scaremongering from GCHQ and the major suppliers who want the Government to spend ever more money on cyber-war preparations and on surveillance. As for the reality of the threats, we refer the Committee once more to our report.
4. The Committee's third topic is "the effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change". As our report makes clear, most of the global law-enforcement response to cybercrime is in the USA, and the rest of the world tends to free ride. The reasons are easy enough to understand and follow directly from cyber-crime's global nature. Suppose a bad man in St Petersburg sends out a million phishing emails; as London is 1% of the Internet, the Commissioner of the Met will see 10,000 of them in his manor. He will be tempted to say "The FBI will have seen 200,000 of these; let them deal with it." This classic public goods problem has made it very difficult to sustain cyber-crime enforcement activities in the UK (and in most other countries). Things are made more complex in Britain by the capture of some crime-fighting resources by particular interests; for example, the banks pay most of the budget of the Dedicated Plastic Card and Cheque Unit, which is unsurprisingly perceived to be reluctant to investigate insider frauds seriously.
5. The Committee than asks "whether there are any gaps in the response to e-crime and, if so, how they should be addressed". The top priority should be arresting cyber-criminals and putting them in jail. A lot of economic damage is done by a small number of gangs, yet many police forces throw up their hands and assume it's all too difficult. Government has from time to time advocated that users take more care, or that people buy more anti-virus software. Yet these measures are ineffective, inefficient or both (see 7 below). A small additional effort in enforcement could yield much bigger returns. The Government should have given more of the cyber-security budget to the police, and less to GCHQ.
6. The Committee wants "options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use". When bad things happen to citizens online, the material harm that results usually amounts to disputed transactions on the citizen's bank or credit-card account. The biggest failing in the UK, of those which could be tackled by legislative means, is in bank regulation: specifically poor consumer protection, the incompetence and indifference of the FSA, and the fact the Financial Ombudsman Service is not up to dealing with the consequences of online and electronic fraud. The problem is not, as is sometimes said, a matter of the burden of proof. British banks found that they could get away with dumping much of the liability for fraud on the customer, by asserting in disputes that their system provided evidence that carried the day on the balance of probabilities. That assertion is routinely accepted by the Ombudsman, and cannot easily be challenged by the customer for want of access to the banks' systems for expert examination. The few customers with the stomach and resources to

[14] See http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

make a fight of it in the courts have often found that the bank fold, in order to avoid a precedent, but this has not helped the others. The banks' greed was exacerbated by ministers' decision to have people report fraud to the banks rather than the police, in order to minimise the fraud statistics. What Parliament might usefully do here is to hold hearings into the failures of the FSA and the Ombudsman. This could document the problems: citizens have suffered, and the UK has failed to meet its international obligations, in that the Payment Services Directive has not been adequately implemented.

7. The Committee finally asks about "the effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples' online behaviours for related public policy". A number of ministers have in the past claimed that Internet security could be promoted by raising public awareness. This view is also echoed by banks and software vendors—anyone who seeks to externalise liability for poorly designed systems. However the experience of system engineers is that poor design cannot be fixed by "blame and train" as the strategy is known. This strategy does not even work in environments such as aviation, where the users (pilots) are subject to mandatory and regular retraining and recertification; it is accepted that when safety hazards arise from poor cockpit design, the vendors must change the design rather than blaming pilots for the resulting accidents. It is even less likely to work in the world of consumer electronics and online services, where vendors no longer ship manuals with their products; users are expected to learn to use them through exploration. And while knowledgeable users might mitigate risks, vendors and system operators usually push the wrong way. For example, a good rule for naïve Internet users would be "if you get to a website by clicking on a link, don't even think of entering a bank password there. If you want to do bank transactions, always go to your bank using a browser bookmark or by typing in the URL directly." Yet bank marketing departments deluge customers with marketing emails which entreat them to click on links. Against this marketing barrage, government PR can achieve nothing. Legislators should merely ensure that if banks' poorly-designed systems and risk-encouraging marketing programmes lead to customers losing money to phishing attacks, then the customers must be made good.

Ross Anderson FRS FREng
Professor of Security Engineering, Cambridge University
Chair, Foundation for Information Policy Research

Supplementary written evidence submitted by the Foundation for Information Policy Research [EC 06a]

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We refer to the evidence I gave to your inquiry on 20 December and the subsequent letter from the banks' trade association Financial Fraud Action (FFA) to the Chairman, the Right Honourable Keith Vaz MP, of 29 January this year. We would like to offer the following observations and suggest a few questions for the FFA witness.

1. The FFA's Ms Worobec objects to my remark to you that banks find it easy to blame customers for fraud, and often blame people as a routine matter, even when there is no evidence of negligence at all.
2. Ms Worobec claims that "the innocent victims of fraud can expect to receive full protection against any losses … it is only in circumstances where customers have been grossly negligent in protecting their PIN and card that they sustain any loss—which is a high threshold to overcome".
3. This has been the line taken by the banking industry since at least 1994 but it is at variance with both the statistical evidence and the facts of many cases.
4. I was recently the expert witness for the defence of Mr W, a national of Sri Lanka who has been granted asylum in the UK. He disputed 38 transactions totaling £7,861.85 on his account at the Nationwide. The Nationwide claimed that according to their records his card and PIN had been used so he must have been negligent or complicit. When he complained, he was arrested for fraud by false representation; the police believed the bank's claim that fraud was not possible. I submitted an expert witness report showing how fraud was indeed possible and the case collapsed. My report described how the bank's fraud analyst, on whom the police relied, had made more than one untrue statement. However Mr W has not been reimbursed; and he also lost his job as a consequence of being arrested. Honourable members might ask Mr Worobec whether she will get the Nationwide to refund and compensate Mr W. (I have his permission to send you the papers so long as his name is not published.)

5. My colleagues and I at Cambridge University Computer Lab have published most of the academic research on payment fraud over the last 20 years, so victims often find us when they search online and come to us with their stories. It is thankfully rare for a complaining cardholder to be actually prosecuted (Mr W is only the third we've come across in 18 years, and all three were acquitted). But it is extremely common for cardholders to be told "Our records show that your card and PIN were used, so you must have been negligent or complicit".

6. The steady stream of victims is scientifically useful as it enables us to see how fraud tools and methods are developing. In the last five years we have seen and documented a number of clever technical frauds that enable card data to be captured from tampered terminals, and which even enable stolen cards to be used without knowledge of the PIN. The fact that a bank's records claim that the correct PIN was used usually proves nothing of the sort. We have a series of technical papers and videos on fraud methods available online.[15]

7. But the stream of victims is also frustrating and at times heart-rending, as there is often little we can do. Given current rules on legal aid and costs, and given that he does not speak good enough English to act as a litigant in person, Mr W seems to have little chance of getting his money back.

8. In general the victims who come to us having been given the brush-off by the banks and then by the Financial Ombudsman Service are disproportionately less white, less male and less middle-class than the population as a whole. They are precisely those people who are not in a position to take the bank to court.

9. The police are usually not much help either, especially since an ACPO decision in 2005 to get people to report fraud to their bank in the first instance rather than to the police. The House of Lords Science and Technology Committee examined "Personal Internet Security" in 2008; their Lordships concluded that that decision had been the wrong one. Yet they could not get ministers to change their minds.

10. So the only really dependable fraud figures appear to be those from victim surveys, such as those conducted by the British Crime Survey and Eurostat, mentioned in our original submission to the committee. These suggest that about 4% of the population become fraud victims in any year and about half don't get their money back. What's more, the fear of online crime is real and it discourages many people from doing more things online, causing real harm to the economy.

11. Ms Worobec talks of the Financial Ombudsman Service (FOS). Yet this routinely finds in favour of the bank and against its customer, even when this flied in the face of both the law and the facts. FIPR made a submission to this effect to the review of the ombudsman that was conducted in 2008, before the ombudsman became the adjudicator required by the Payment Services Directive.

12. In that submission[16] we included the full papers of a sadly typical case. Donald and Hazel Reddell were intimidated by Barclaycard into paying up £3000 that had been stolen from their account after their card was cloned—on the single occasion when they used it, namely in a Barclays Bank ATM! The bank showed its confidence in the Ombudsman by sending in the debt collectors in while that august body's formalities were still in progress. Donald and Hazel appeared on "Tonight with Trevor McDonald"; I raised their case with a nonexecutive director of Barclays; I wrote to Bob Diamond after he made a speech saying the bank would have to rediscover its ethics; and I even put their case before the bank's much-heralded Salz review. Yet despite a complete lack of evidence of any contributory negligence on their part, Barclays have still not given the Reddells their money back. I suggest that honourable members ask Ms Worobec when the Reddells will receive their refund. They can hardly be described as "having practically colluded with the fraudster".

13. Ms Worobec also talks of the Payment Services Regulations 2009, which transpose the Payment Services Directive. I would like to draw the committee's attention to article 59.2 of the Directive: "*Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56.*" The UK banking industry lobbied long and hard to get the word "necessarily" inserted into this text. I invite the committee to ask Ms Worobec why. Was it not so that UK banks could continue saying "Your card and PIN were used so you must have been negligent or complicit"?

14. Indeed as recently as a year ago, complainants to the Ombudsman reported that adjudicators there had not even heard of the Payment Services Regulations. We wrote to the Business Secretary Vince Cable (having discussed the matter with him while he was in opposition); his response was that he could do nothing as the ombudsman was "independent", but that we might see the FSA who assumed the power to regulate her as of April 1st. We met with the FSA in

[15] Bank fraud resource page, at http://www.cl.cam.ac.uk/~rja14/banksec.html

[16] FIPR submission to the Hunt Review of the Financial Ombudsman Service, 2008; at http://www.fipr.org/080116huntreview.pdf

January but learned that despite the ombudsman's manifest failings they did not propose to do anything about her at all. Their line is that "the basis for Ombudsman decisions is what is fair and reasonable in all the circumstances of the case, rather than on a strict legal basis". We disagree; if the ombudsman service does not have to follow the PSRs and the rest of the law (including the Human Rights Act) then the UK does not have an adequate transposition of the Payment Services Directive.

15. NGO efforts towards securing better financial consumer protection in the UK are now aimed at persuading the European Commission to remove the word "necessarily" from the Payment Services Directive in the current review of that legislation, and require explicitly that adjudicators act according to law. The committee might ask Ms Worobec whether UK banks will resist either or both of these changes.

16. Yet, despite its serious flaws, the Financial Ombudsman Service is finding against the bank in tens of thousands of cases per year. In 2012 there were 64,234 complaints to the ombudsman regarding banking and credit[17]; 31% of these for current accounts and 54% of these for credit cards were found against the bank. The figures are not broken down enough to give the phantom withdrawal figures, but it is clear the banks' system for refunding customers is not working.

17. So I am delighted to see Ms Worobec claim that 98% of fraud victims are reimbursed. I encourage the committee to ask her to provide the data from which this figure was derived. 98% of what, precisely?

18. The committee should be aware that when customers complain of transactions that are "chip and pin" (according to bank records) some banks see these simply as attempted frauds where the bank was the victim, not the cardholder, and record them under another heading. If customers are told to go away as "Our systems are secure so you must have been negligent or complicit", a complaint may not be recorded at all. And a third example of non-recording is where the bank claims the dispute is purely between the cardholder and a merchant; the line is that where there was a "willing buyer and willing seller" the dispute does not concern them. A common example is where a British tourist in southern or eastern Europe gets a large card bill after eating in a restaurant where a waiter made a copy of their card and cashed it out in a nearby nightclub. UK banks then hide behind card scheme refund rules (which we understand even the FSA are not allowed to see). UK banks' unwillingness to file chargebacks even for clearly fraudulent transactions encourages crime gangs in other countries. You might ask Ms Worobec whether eating tapas in Spain amounts to "having practically colluded with the fraudster".

19. Ms Worobec claims that the burden of proof is on the bank, not the customer. This is somewhat disingenuous. The problem is that the fact that the banks assert that their system provides evidence that carries the day on the balance of probabilities. The ombudsman accepts this; it cannot easily be challenged by an ordinary customer for want of being able to get access to the banks' systems for expert examination; and the courts do not usually order wholesale disclosure because there is so much of it that such an order would never be proportionate to an ordinary civil case. Where disclosure is ordered in a criminal matter (as in Mr W's case), or where a fraud victim has the stomach and resources to make a fight of it in the courts, the banks fold. But ordinary fraud victims have little chance.

20. A matter that Ms Worobec failed to mention in her letter is that after colleagues and I revealed how stolen cards could be used by a criminal who did not know the PIN on Newsnight in February 2010, her colleague Melanie Johnson wrote to the University of Cambridge asking for one of our students' Masters thesis to be removed from the web. The banks claimed it might help the bad guys, but this was nonsense. We had found that vulnerability after studying fraud patterns; the villains knew how to do it already. Ms Johnson appears to have simply been trying to defend the industry line that "Our systems are secure so you must be negligent or complicit". We made her go away by pointing out to her that section 2 of the Fraud Act 2006 makes it an offence to dishonestly make a false representation to benefit yourself or another, or to put a third party at risk of loss. But perhaps many people who work in the banking industry still imagine that this law applies only to poor people like Mr W, and not to them.

Ross Anderson FRS FREng
Professor of Security Engineering, Cambridge University
Chair, Foundation for Information Policy Research

April 2013

[17] Financial Ombudsman Service, Annual review 2011/2; at http://www.financial-ombudsman.org.uk/publications/ar12/about.html#a2 and /dealt.html#a5

Written evidence submitted by the City of London Police [EC 07]

SUBMITTED BY THE OFFICE OF THE CITY REMEMBRANCER

1. *Introduction*

1.1 The internet has revolutionised society, and provided communities and business with great opportunities, and usage is set for a further prodigious increase over the next few years. The internet has encouraged and assisted new businesses by promoting innovation and the sharing of ideas, which has also boosted both the economy and job growth. It has allowed businesses to lower their costs, promote their brand and increase efficiency, and gives customers immeasurable choice and access to better, cheaper and more convenient services. The UK economy is very dependent on the internet as a basis for business and communications which is exemplified by the fact that in 2010, three quarters of UK consumers shopped online, spending nearly £60 billion, while 42% of all UK adults bank online.

1.2 These benefits, however, also provide opportunities for criminals. It allows them to exploit new ideas for fraud, identity theft, intellectual property theft and other forms of crime on an unprecedented scale through access to victims, data and commodities. They have done this by using a variety of cyber tools, techniques and online services. Criminals also utilise international boundaries to develop inventive and complex infrastructures that enable them to commit e-Crime. They have done this by using a variety of cyber tools, techniques and online services. Criminals are also adopting new technology to enhance their operational security or improve the efficiency of their operations.

1.3 The City of London Police (CoLP) has led the implementation of the National Fraud Intelligence Bureau (NFIB) since 2010. Prior to this, due to its unique relationships with the financial community in the City and the specialist fraud investigations skills and experience of its detectives, the City Police had been designated the National “Lead (Police) Force (NLF)” for fraud since 2003. The force receives additional funding from the Home Office to investigate serious and complex fraud and also to run the National Fraud Intelligence Bureau. These fraud functions come together as the Force’s Economic Crime Directorate (ECD) and are match funded by the City of London Corporation. Within policing, the force leads the Association of Chief Police Officers (ACPO) Economic Crime Portfolio and has been working with Chief Constables across the country over the passed 12 months to define a new model for recording and investigating fraud.

1.4 The NLF provides specialist advice on law enforcement dealing with often highly complicated and detailed criminality. Its objectives are to provide advice to all police forces, industry investigators and other law enforcement agencies to disseminate best practice, deliver training and act in an independent advisory capacity to other forces on request. The NLF provides a national investigative capacity to deal with all types of fraud (subject to agreed case acceptance criteria) and to assist other police forces in local investigations, and act as a single point of contact for anti-fraud advice.

1.5 As a result of the Fraud Review in 2006, the concept of the National Fraud Intelligence Bureau (NFIB) was created along with Action Fraud (the brand name of the National Fraud Reporting Centre launched and run by the National Fraud Authority) to help UK law enforcement agencies and their partners catch and disrupt criminals and to alert communities to fraud threats. The NFIB gathers a large volume of information on suspected fraud from both public and private sector sources, much of which is not reported to, or made routinely accessible to the police. This is analysed and turned into intelligence such as the identification of the scale of fraudsters’ criminal activities. The intelligence is used to support law enforcement operations and also provide prevention advice to industry.

1.6 The Government’s National Security Strategy, published in 2010, ranked UK cyber security (of which e-Crime is an element) as a Tier 1 national security priority. As a result of this threat, the Government has committed £650 million to the National Cyber Security Programme (NCSP). The City Police is one of a number of organisations that has received funding to help deliver this programme.

1.7 At the end of 2011, the Government published its Cyber Security Strategy, which illustrated how the UK will support the economy; protect national security and safeguard communities by building a secure and resilient digital environment.

2. *What is e-Crime understood to be and how does this affect crime recording?*

Types of e-Crime

2.1 The NFIB sees e-Crime (also variously described as internet crime, cyber crime and technology enabled crime) at two levels. At the simplest level, it is crime that exists only because of computer technology, for example hacking of email accounts, denial of service attacks and the production and deployment of malicious software (“malware”). These offences are largely covered by the Computer Misuse Act 1990. Additionally, there is “electronic” or cyber-enabled crime which can be described as the use of the internet to enable other crimes to be committed. The latter features particularly strongly within the NFIB’s remit as cyber enabled fraud. The most damaging cyber enabled frauds are those where the ease of communications through the internet has allowed an existing type of fraud to be attempted much more easily (for example, advanced fee or

"419 letter"[18] frauds have developed and grown into fraud perpetrated by "phishing"[19] emails) or frauds exploiting the methods of genuine e-business such as ticketing fraud using bogus websites or online shopping fraud.

2.2 The bulk of e-Crime data that NFIB assesses is received from Action Fraud. Action Fraud records crime aligned to the Home Office Counting Rules for Fraud and Forgery, which includes crimes committed under the Computer Misuse Act 1990. However the reports it receives at present are limited to individual calls or reports from the public. Police forces still represent the bulk reporting for fraud and the service recognises that through the complex method of cyber crime and also because of jurisdictional issues, victims can receive a very different service depending on how or where they report their crime. Chief Constables have therefore agreed to a new business model lead by the City of London Police which will involve a national reporting and case allocation model to offer victims, a more professional service.

Recording

2.3 The recording of crime by the police is governed by the National Crime Recording Standard (NCRS) and the Home Office Counting Rules (HOCR). These set out the principles under which reports received from victims are recorded. Crime statistics that are recorded by police are based on a notifiable list of offences. The HOCR set out the classification groups into which offences are managed for statistical purposes.

2.4 However, individual police forces record crimes, particularly those enabled by technology, in different ways. This is because there is no such crime type as an "e-Crime" formally defined in legislation. The use of a computer or other cyber technology is an enabler to the crime, and not a crime type in its own right. Therefore, it is not centrally recorded. This presents difficulties to the law enforcement community in assessing the scale and nature of the e-Crime threat.

2.5 The City of London Police is currently leading a programme of work to introduce Action Fraud reporting to all police forces in England and Wales. This will reduce some of the issues created by the lack of harmonisation that currently exists by creating a national call centre and on line facility to report fraud and cyber crime.

2.6 Over the coming months, Action Fraud, in partnership with the National Fraud Intelligence Bureau, will press ahead with the "roll out" of an improved crime reporting capability with the support of all UK police forces. Within this programme is the development of an enhanced reporting method for businesses who are victims of cyber crime. This will ensure the police, through the NFIB, will have the capacity and capability to analyse all fraud and cyber crime data from one source, allowing for a much better understanding of the extent and nature of the e-Crime threat, and also provide for an enhanced service to victims.

2.7 New crime recording classifications have also been introduced by the Home Office to enable law enforcement agencies to capture specific cyber crime offences as laid out in the Computer Misuse Act (1990), but many crimes committed online are also prosecuted under existing legislation such as the Fraud Act (2006) or the Communications Act (2003).

3. *What is the extent and the nature of the threats on which e-crime policy is based?*

3.1 The significance of cyber criminals has grown in line with the development of online technology and the proliferation of electronically held data. Although it is difficult to estimate accurately the scale of losses to the UK economy as a result of e-Crime, one report puts the figure at £27 billion per year.[20] Whatever the true cost, its reach is known to be extensive, affecting individuals, businesses and government institutions.

3.2 The Government has expressed the need for partnership with the private sector and academia to combat crime. The City of London Police enjoy close working relationships with the private sector (who are represented at the ACPO Economic Crime Portfolio meetings), through private data sharing agreements with the NFIB and also through industry funded police investigation units such as the Insurance and Cheque Fraud investigation units. There is a very clear common message concerning the co-ordination of engagement with the private sector across government. Whilst government policy has provided a useful high level perspective, they have only resulted in bespoke isolated programmes of engagement and there are still no clearly identified "nodes" for the formulation of policy, strategic forecasting and operational collaboration with the private sector on a national scale. Given this confused picture, there may be merit in an initial "mapping" exercise to identify the optimal mechanisms for engagement that already cut across different government departments.

3.3 The rapid pace of change in terms of technology and techniques used by cyber criminals make mitigating e-Crime a unique challenge. The ever-increasing amount of public and private data held online and the significant increase of internet usage, both privately and commercially, also allows for an increase in opportunities for criminals to exploit weaknesses. Further evidence of the threat posed was illustrated in a BBC

[18] This type of fraud is a commonly attempted fraud whereby victims are asked to help transfer money out of another country—such as Iraq, South Africa or West Africa—by paying a fee in advance. In return, the victim is promised a percentage of the money that the fraudster says will be transferred.

[19] Phishing is attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an email.

[20] *The Cost of Cyber Crime*, Detica (for The Cabinet Office), February 2011

report in July 2012,[21] which shows fraudsters traded 12 million pieces of stolen personal information online between January and April 2012. The figure represents a threefold increase on 2010. Credit-checking company Experian, which produced the figures, said the increase was partly due to consumers having a growing number of online accounts. Consumers now have an average of 26 separate online logins but just five different passwords. Experian said many people were unaware their identity had been stolen until they were refused credit cards or phone contracts.

3.4 Attacks on businesses have risen markedly over the past year, with most UK based companies reporting malicious software infections. The 2010 Information Security Breaches Survey[22] found that 90% of "large" organisations and 74% of "small" organisations had experienced a malicious security incident within the last year, including hacking, viruses, data theft and fraud.

3.5 In August 2011, Action Fraud launched the capability to record the enablers of fraud within fraud reporting. Since August to the end of the financial year, the NFIB have received a total of 49,037 fraud and internet crime reports from Action Fraud of which 45% were enabled[23] online.[24] The highest volume of frauds reported to Action Fraud are concerned with online shopping and auctions, many of which are linked to organised crime. As an indication of the scale of only one aspect of e-Crime, over 25,000 "phishing" emails were forwarded by members of the public to the NFIB in less than one week during the Office of Fair Trading's SCAMNESTY campaign. The majority of traditional frauds have been eclipsed by an internet enabled variant and all forms of legitimate internet commerce are vulnerable.

3.6 In considering the impact of e-Crime, the experience and effect on fraud victims has also to be considered. It is the experience of the City of London Police, that, a large number of victims have found fraud to be as harmful to them as violent crime, with tens of thousands of victims requiring medical intervention for psychological and physical stress related injury each year as a direct result of being defrauded.

4. *What is the effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and what are the potential impacts of proposed organisational change?*

Are there any gaps in the response to e-crime and, if so, how should they be addressed?

Effectiveness of current law enforcement and legislative capabilities

4.1 The Serious and Organised Crime Agency (SOCA) and the Police Central e-Crime Unit (PCeU), hosted by the Metropolitan Police Service, undertake national e-Crime investigation and international joint investigation. The introduction of the new National Crime Agency (NCA) in 2013, which will replace SOCA, will continue with and expand on this role. Whilst the NCA is not yet operationally effective, the activity and linkage currently being initiated in the build up to the 2013 start date indicates that the operational response will be enhanced. Within the Shadow Command of the NCA, the City of London Police is member of the Economic Crime Coordination Board (ECCB) and also supports the three sub groups; Prevention, Intelligence and Enforcement. Early pathfinder joint operations have targeted criminals who are using the internet to facilitate money laundering and fraud.

4.2 The development of the partnership and coordinating functions of the National Cyber Crime Unit (NCCU) being established within the NCA will also provide a better-coordinated and standardised approach to the e-Crime threat. Many of the concerns and issues will, in part, be addressed by the unit, which draws together and adds to the work currently carried out by SOCA's Cyber Unit and the PCeU.

4.3 The NCCU will focus its resources and skills on the most sophisticated areas of cyber crime, whilst supporting the NCA and wider law enforcement to take responsibility for tackling cyber-enabled crime. This principle of supporting law enforcement to take responsibility for tackling cyber-enabled crime will underpin the work of the NCCU. Cyber crime that is facilitated by the internet will continue to be investigated by the police.

4.4 The creation of the NCCU is a critical part of the Government's wider National Cyber Security Programme (NCSP). It will consolidate the national law enforcement response to cyber crime into one unit. The NCCU will work closely with other partners to strengthen the UK's overall response to e-Crime and ensure individuals and industry can utilise the opportunities presented by the internet. The NCCU is responsible for building the cyber capability of the NCA, across all four operational commands to manage high impact incidents of cyber and cyber-enabled crime.

4.5 An improved response to e-Crime can also be seen with the development of the Cyber Crime Threat Reduction Board (TRB), and of the Fraud Threat Reduction Board. These were established under the Government's organised crime strategy[25] which provides an operational context in which law enforcement

[21] "*Warning about online fraud as information theft rises*", BBC News Website, 17 July 2012, http://www.bbc.co.uk/news/technology-18866347

[22] *The Information Security Breaches Survey 2010*, PwC, April 2010

[23] Reporting consists of both crime and information reporting; either by the nature of the offence ie, online shopping and auction fraud, hacking, etc or as had been selected by the victim during the reporting process.

[24] It is believed the true proportion of internet enabled fraud is higher than this as an accurate assessment depends on the victims correctly knowing, identifying and recording an enabler when reporting the crime

[25] *Local to Global: Reducing the Risk from Organised Crime*, Home Office, July 2011.

and intelligence agencies can assess operational and intelligence activity against the "Stem, Strengthen and Safeguard" themes of the Organised Crime Strategy. Both of these boards bring together representatives from key organisations to tackle specific issues within their remit, with a partnership-based approach. Whilst only recently established, both TRBs have already made significant progress, assisted by the Threat Reduction Assurance Forum, which oversees and links the work of both these boards, alongside the other seven TRBs responsible for their respective crime types. The Threat Reduction Action Plans, identified and implemented on a bespoke basis by both boards, ensures clarity, effectiveness and coordination for the first time.

4.6 The ECCB has also produced several significant products in 2012 that have allowed a greater understanding of the fraud threat, identified gaps in knowledge, and highlighted key threats and risks. The intelligence gap analysis report and Strategic Threat Assessment are now being used to inform the formulating of a Control Strategy to manage economic crime nationally in a coordinated, effective and efficient way. These products incorporate e-Crime.

4.7 A significant amount of e-Crime is also the responsibility of the NFIB, and the police service as a whole. This has resource and capability implications as it lands alongside other priorities as part of the general demand on policing. As an intelligence bureau, the NFIB assesses the crimes it receives and then distributes them to the appropriate police force or law enforcement agency for investigation; this can include PCeU and SOCA. In reality, due to competing priorities, and the complexity and resources often required, many police forces have difficulty in investigating e-Crime.[26]

4.8 Police forces across England and Wales are faced with a 20% reduction in national funding in the period 2011–2014. This means that resources for targeting financial crime, including much e-Crime are likely to be reduced in some regions. The City of London Police has proposed a joint funding initiative with the Government and the banking sector to fund additional police resources in the 10 ACPO police regions to investigate fraud, a great proportion of which is now conducted through the internet. These resources would complement the existing regional units that investigate organised crime and asset recovery, and would also be closely aligned to the NCA build, including the specialist PCeU resources. Initial first year funding has been approved by the Home Office, resulting in intelligence officers being deployed in the 10 ACPO regions, to liaise with the NFIB and assist further in identifying and understanding the associated regional fraud threats. If further funding for an additional two years is approved, the intelligence officers will work alongside new regional fraud enforcement teams to provide a comprehensive intelligence-led response on a regional to national level.

4.9 Whilst individual police forces do provide a local response to e-Crime, this can be uncoordinated and inconsistent, with many factors impacting on a variable policing response from region to region. A project has been developed by PCeU to provide additional regional resources that are effectively trained and equipped. The National e-Crime Programme has delivered three pilot PCeU "hubs" to address a lack of regional focus. The "hubs" enhance existing PCeU national operational capability to respond and investigate cyber crime. The regional "hubs" are based in the North West, East Midlands and Yorkshire & the Humber. The "hubs" were launched in February 2012 and are already providing a fast and effective response. The PCeU "hubs" have enhanced the local policing response but further dedicated resources are still required to investigate the underlying fraud offences.

4.10 The publication of the Strategic Policing Requirement (SPR) will support national co-ordination and collaboration between police forces to respond to serious and cross-border criminality. The SPR is also intended to ensure local policing plans account for cyber capability, and that local police forces can access the necessary specialist services required.

4.11 The introduction of Police and Crime Commissioners (PCCs) in late 2012 is intended to provide strong local representation, with the PCCs able to set the priorities for the police force within their force area, respond to the needs and demands of their communities more effectively, set the force budget and priorities, and hold the local Chief Officer to account for delivery and performance. With the extent of internet enabled crime effecting local communities, fraud and e-Crime should be seen as a serious and growing problem that needs to be addressed.

Gaps in response to e-Crime

4.12 The greatest challenge to an effective response by UK law enforcement agencies is the globalised nature of the threat. The most effective e-Crime groups are organisations that operate internationally, separating the component parts of their criminal enterprise across different countries for their utility and selecting jurisdictions for their permissiveness. There are challenges associated with delivering an effective solution in this environment due to the current varying international police response and enforcement. Differences in legislative, regulatory and practical arrangements for managing cyber security have potentially serious implications for all organisations. Whilst there is not necessarily the need for new international legislation, the promotion of standards and norms could help to strengthen the global threat mitigation architecture. Lessons can be learned from examining best practice in some sectors, and from the experiences of international partners. There is also a need to consider intelligence requirements through a global perspective.

[26] Due to investigative capacity, the difficulty in identifying the criminals behind e-Crime and the jurisdictional challenges of dealing with criminals who are frequently located outside of the UK.

4.13 In addressing the issue of e-Crime, the use of terminology needs to be clearer and more consistently used. There is a requirement for a common understanding of some of the general terms and an agreed list of the cyber crime techniques and tools, and the criminal infrastructure that poses the most risk to the UK. Both public and private sectors are the victims of cyber crime, but these are very wide categories and in the first instance prioritisation should be given to specific parts within these sectors that face the most risk and harm. A common understanding of terminology both in terms of threats and mitigation is a vital component of the UK response.

4.14 The current challenges in assessing the scale and nature of the UK e-Crime threat affects both the policy around e-Crime and the operational response to it.[27] The impact of this is magnified by the tendency of cyber criminals to be highly adaptive and innovative. As a result, they can often be a few steps ahead of the law enforcement community's ability to respond and are often in the process of exploiting the next criminal opportunity whilst law enforcement is trying to target the previous one. An effective law enforcement response is challenged further by the need for many industries to harness new technology to enable a more efficient and effective service. For example, new payment technologies and alternative banking mechanisms are rapidly evolving both in the UK and overseas. In a highly competitive market, the desire (and need) to generate new products rapidly makes delivering comprehensive security controls for these products a formidable challenge. Many organisations' decision-making in relation to innovation is heavily driven by market forces and ease of use, with security concerns sometimes taking second place.

4.15 Key risk areas that need to be prioritised for affirmative action include online tax and benefit/tax credit systems (Universal Credit) in the public sector, banking and payments and retail (the UK has the second largest in the world) for the private sector, and personal computers and devices used to access public and private sector systems. The means by which these systems are accessed are often the weak links which cyber criminals attack. Government has a key role to play in working with the private sector to mitigate the threat posed by these systems.

5. *How effective are current initiatives to promote awareness of using the internet safely and what are the implications of peoples' online behaviours for related public policy?*

5.1 Whilst the UK has seen some recent initiatives to promote awareness of internet safety, it is clear that more needs to be done within this area.

5.2 Through its regional hubs, the PCeU have worked hard to mainstream cyber awareness, capacity and capability since its inception.

5.3 The National Fraud Authority (NFA) as part of the "Shadow" NCA—ECCB Prevention Sub Group, plays a key national preventative role, in terms of reducing repeat victimisation by advising callers to Action Fraud. This service also plays a vital role for crime victims by offering reassurance and other advice through a bespoke service in partnership with Victim Support. The NFA also initiated and developed the "Devil's in Your Detail" campaign, a joint initiative between the NFA and private sector organisations from the banking and telecoms industries. The campaign was video-driven and raised awareness of the importance of protecting personal information. The campaign reached over four million people through initiatives involving social media. Subsequent analysis of 4,000 people who watched the videos resulted in over 60% stating that they would take more steps to protect themselves from fraud.

6. *What are the options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use?*

6.1 The key to addressing e-Crime effectively is through greater collaboration, effective intelligence sharing, improved engagement with business, and a comprehensive awareness programme. Prevention is a vital theme that threads through all of these areas.

Greater Collaboration

6.2 The Government's National Cyber Security Strategy makes clear, and this is applicable to information security in general, that it is only through engagement between government, law enforcement and the private sector that the UK will become more resilient from attack, shaping an open and stable environment and developing our skills base. As criminals will target a range of industries it will be vital for all sectors to come together to share experiences and develop common strategies for addressing threats. A particular focus must lie in the security of the millions of personal information records held by both the public and private sector. There is a wealth of intelligence from various sources that this data is being targeted, stolen and traded as a commodity by criminal gangs. A comprehensive approach to the threat is required and collaboration is the key to success. Ad hoc groups promoting collaboration across the sectors do exist however, there is a need for a stronger coordinated and formalised process across both the public and private sectors.

6.3 Collaboration can come in many forms, and the proposed City of London Police joint funding initiative to provide a national policing capability for fraud would provide a very effective specialist resource, aligned

[27] Response tends to be reactive rather than proactive and strategically targeted

to the national law enforcement picture on a local, regional and national basis, and tackling an area of crime that has had limited resources. Whilst already supported by ACPO and all police chiefs, such a venture needs the financial support of the Government and the banking sector. Whilst the three-year pilot requires investment, the benefits to potential supporters, and the UK as a whole, are expected to be commensurately higher.

6.4 Criminals may target third parties, partner companies and other industries to access data. Advances in technology, such as the development of Cloud Computing, are also a source of new risk as well as opportunity. There is a wealth of expertise and information across all sectors in the UK that could greatly enhance protection against such wide-ranging threats, and collaboration must be co-ordinated across the wider private sector and government. To facilitate such comprehensive co-ordination and collaboration, there is a need for a point of focus around which stakeholders can rally.

Improved intelligence sharing

6.5 An improved and more effective intelligence sharing protocol between law enforcement agencies would also have a great impact on preventing e-Crime. There is still much to be done in this area, and many agencies could collaborate and share their intelligence more effectively. The fact they are not is due to many reasons, including cost, culture, and their respective regulations, but none are insurmountable, and a greater effort is required from all agencies to share the intelligence they possess.

6.6 The National Fraud Intelligence Bureau (NFIB) is an example where intelligence sharing can lead to an effective preventative response. It disseminates products, including alerts, as a result of analysing intelligence provided by a range of organisations and industry sectors. This collaborative approach has been extended further with some also providing staff to work within the bureau. The NFIB works with private sector partners to close down criminally managed websites. Between January to April 2012, 261 websites were sent for suspension request. Between April to August 2012, 52 websites have been confirmed as suspended. In September 2012, 152 have been sent for suspension, with 143 being confirmed as suspended. Between January to August 2012, 248 telephone numbers were identified for suspension. The submission of bank account alerts was instigated from April 2012 and since this date 221 account details have been disseminated to the banking industry in 177 alerts. These are sent to the banking industry for intelligence purposes, and an example of the impact that these alerts provide was when a single customer had £70,000 prevented from being defrauded in September 2012. These timely actions are calculated to have saved the finance sector millions of pounds.

6.7 In May 2012 alone, the NFIB developed and disseminated 449 crime investigation packages, 28 tactical intelligence products and 112 alerts via a new partnership with the British Bankers Association. Whilst the work of the NFIB encompasses all areas of fraud, this approach should be expanded upon, and further supported, to encourage greater intelligence sharing of e-Crime related threats.

Engagement with business

6.8 The majority of victims of banking and plastic card fraud are protected by compensation from the finance and banking industry. Whilst much is done within this sector, the industry needs to continue to be supported and encouraged to provide enhanced and effective security to mitigate the ever changing and often innovative exploitation by criminals and criminal finance. A robust coordinated approach by Government, law enforcement and business will ensure a better understanding of the true level of crime and raise public awareness to the threat and how to reduce it.

Education

6.9 The safe use of the internet requires a continuous, pervasive and constantly updated approach to education. This needs to be mainstreamed throughout an individual’s lifetime education. This would need to be on the scale of other public safety education, such as road safety and “stranger danger”, with initiatives seeking message adoption and understanding through all sectors of society. Although public awareness of “cyber enabled fraud” has greatly improved (for example the significant amount of education built into the school curriculum to manage children’s online behaviour by the Child Exploitation and Online Protection Centre), increasingly sophisticated attacks continue to target home computer users, and much more coordinated work is required.

October 2012

Written evidence submitted by EMC and RSA [EC 08]

Introduction

1. EMC welcomes the opportunity to contribute to the Home Affairs Select Committee's important and timely enquiry into e-crime. This response begins with an executive summary followed by a short introduction to EMC, its global reach, and its expertise and capabilities in cyber security, before addressing the committee's specific questions.

Executive Summary

— EMC is one of the world's major IT infrastructure and services providers and has a significant presence in the cyber security market through its RSA division.

— The cyber-crime threat is sophisticated, complex, and rapidly evolving. There is a thriving criminal ecosystem that mirrors the legitimate IT market where criminals can freely buy and sell malicious software and services. This rapidly maturing online black market has led to a tenfold reduction in the cost to access cyber crime tools and services and an increase in the volume and sophistication of attacks seen.

— If the UK online environment is to remain safe for citizens, as well as the public and private sectors, there must be continued and increasing efforts to raise awareness of the extent and rapidly evolving nature of the e-crime threat, both in terms of the actors involved and the new threat vectors they are developing. Intelligence must also be shared and best practice spread in a two-way process involving both the public and private sector.

— In this era of tight budgets and rapidly evolving threats, new regulations stipulating particular technologies or practices to address cyber threats are not necessarily required, or indeed appropriate. Instead a dynamic, outcome based and technology neutral approach should be encouraged, requiring sectors to collaborate and individual organisations to conduct risk assessments and put appropriate controls in place that are commensurate with the identified risk. In this way organisations will be able to develop and maintain more flexible security programmes, processes, and technologies that can evolve ahead of—or at least alongside—the threat landscape.

About EMC and its Security Division RSA

2. EMC was founded in 1979 and is today one of the world's major IT companies. It has annual turnover of around $20 billion and employs over 54,000 people worldwide, including around 1,650 in the UK.

3. EMC is a global leader in enabling organisations in both the private and public sector transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping organisations store, manage, protect and analyse one of their most valuable assets—information—in a more agile, trusted and cost-efficient way.

4. This journey to cloud computing supports improved information security because organisations are able to replace the disparate and piecemeal legacy IT systems that are so common today with centralised monitoring, management, compliance, and security solutions. In addition, security is being built into the information infrastructure that makes up the foundation for cloud computing including virtualisation and data storage platforms.

5. Another key priority for EMC is "big data" analytics, which refers to the ability to analyse and gain real time insights on vast data sets of unprecedented scale and formats gathered from various sources. EMC's big data division Greenplum provides this capability to leading organisations including T-Mobile and Skype, enabling them to gain real time insights on their business and provide a better service to their customers. EMC is increasingly leveraging its expertise in big data to support information security by providing organisations with real-time access to the entirety of information relevant to the detection of security problems.

6. EMC's security division, RSA, provides security, compliance and risk management solutions for organisations worldwide. RSA helps the world's leading organisations succeed by solving their most complex and sensitive security challenges so they can safely benefit from the tremendous cost and productivity gains of digital technology and the internet.

7. RSA has been driving innovation in the information security industry for over 25 years. Today, RSA protects the identities of over 250 million people around the world, including, in the UK, the online banking customers of nine out the country's top 10 retail banks, more than 800 public sector organisations, and 30 defence and aerospace companies. RSA's technology can be found in BlackBerry devices, PlayStation games consoles, and checks more than five billion URLs per day for malicious activity.

Response to Specific Questions

What e-crime is understood to be, and how this affects crime recording

8. To successfully defend against cyber security threats it is important to understand the actors involved better. The attackers can be categorised into three major classes of cyber adversaries: criminals, non-state actors, and nation states. Each has distinct motives and modus operandi but may, at times, collaborate if their goals align. For the purposes of the committee's enquiry, this response focusses on the criminal element.

9. Whether loosely affiliated or tightly organised, cyber criminals are out to steal personal information for financial gain. This information can range from an individual's credit card details and web or corporate logins, to an organisation's highly confidential plans or data. Indeed the value of personal data to a cyber criminal is much higher than a credit card or bank account number alone. For example, the average selling price of a US credit card on the criminal black market is around $1.50. But when that card is sold with a full identity profile, the value can be up to ten times greater.

10. It is typical to see cyber criminals auctioning "on-demand" access to large numbers of infected computers under their control, and knowledge of "zero-day" exploits of previously unknown software vulnerabilities, on the black market to the highest bidder for use in automated cyber-attacks. Indeed criminal groups are able to purchase all manner of malicious software and services online, including "do-it-yourself" kits to create networks of compromised computers ("botnets") that then can be used for the mass distribution of "malware" (malicious software) and benign "bulletproof hosting" environments from which to undertake their activities. Today's malware is incredibly sophisticated—capable of sitting undetected on a user's machine and stealing personal and financial data, taking over accounts, and sending spam emails to proliferate and infect other users.

11. Unfortunately, as the criminal ecosystem matures, the cost of entry for cyber criminals to access these capabilities continues to fall. Research published by RSA in June 2012 found that the rapidly maturing online black market, which mimics functions seen in the legitimate IT supply chain including manufacturing, purchasing, outsourcing, partnerships, development, sales, distribution, performance optimisation, and customer support, has led to a tenfold reduction in the prices being charged for malicious software and services.[28] In 2011, RSA found that roughly one in every 300 emails in circulation contained some element of "phishing", whereby cyber criminals attempt to acquire sensitive information by posing as a legitimate entity, with 50% of these attacks focussed on financial institutions.[29]

12. Although the tools available to cyber criminals are becoming increasingly sophisticated, the preferred method by which they exploit these capabilities centres on people. Security professionals have long understood that IT users will click on links they should not and unwittingly install malware hidden through simple ruses. Security professionals have traditionally deployed multiple perimeter controls, such as anti-virus software, firewalls and intrusion detection systems, to help deal with this threat. This process may work well for generic attacks, but not for the most sophisticated malware or zero-day exploits. For example, the Zeus Trojan, the malware most widely used by criminals to target financial institutions, is detected less than 40% of the time by anti-virus software.

13. Similarly, attackers are increasingly gathering intelligence on their targets, sometimes months in advance of an attack, using social media and other means to understand which individuals possess the assets they want, and crucially how to tailor, or "socially engineer", their attacks to increase their likelihood of success. Indeed cyber attackers prefer using social engineering in this way because in so doing they are able to evade traditional perimeter controls more easily.

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers
The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

14. The tripartite distinction to the cyber threat outlined above appears to be well understood by policy makers and is reflected in the UK National Cyber Security Strategy published in November 2011. However RSA's experience dealing with both the public and private sectors suggests that, while recent policy initiatives such as last year's National Cyber Security Strategy have advanced government's understanding of the cyber threat and how best to respond to it, the private sector remains ahead in terms of understanding its scale and maturity, and implementing appropriate measures to deliver advanced security.

15. Research published by RSA's Anti Fraud Command Centre (AFCC) in July 2012 found that the global volume of phishing attacks seen in the first half of 2012 had increased by 19% compared with the second half of 2011, costing organisations an estimated $687 million in total losses. The UK was among the top 10 countries experiencing phishing attacks over this period.[30]

[28] *Life in the FaaS (Fraud as a Service) Track*, RSA, 12 June 2012, http://www.rsa.com/products/consumer/whitepapers/11794_120612_Life_in_The_FaaS_Track.pdf

[29] *Faces of Fraud 2012 Survey*, Information Security Media Group, http://www.bankinfosecurity.com/p-survey-fraud-2012.

[30] *RSA Monthly Fraud Report*, July 2012, http://www.rsa.com/solutions/consumer_authentication/intelreport/11752_Online_Fraud_report_0712.pdf

16. The AFCC, based in Herzliya, Israel, is one of the most advanced facilities in the world dedicated to fighting international cyber-crime. Established in 2005, the AFCC combines counter-intelligence, threat monitoring, and threat analysis capabilities to neutralise attempts by cyber criminals to steal money and information. Nearly 150 analysts work around the clock, 365 days a year at AFCC, protecting nearly 15,000 private and public sector customers in over 180 countries from cyber security threats and are able to shut down attacks in an industry-record time of five hours.

17. In the first seven years of its operation, AFCC shut down more than 500,000 cyber attacks. But in the first six months of 2012, AFCC shut down an additional 150,000 attacks, at a rate of 1,000 attacks per day. Clearly, the cyber threat is increasing significantly and it is now crucial for all sectors to recognise the dangers involved and respond.

18. If the UK online environment is to remain safe for citizens as well as the public and private sectors, there must be continued and increasing efforts to raise awareness of the extent and rapidly evolving nature of the e-crime threat, both in terms of the actors involved and the new threat vectors they are developing, among senior and mid-level policy makers. Intelligence must also be shared and best practice spread in a two-way process involving both the public and private sector.

19. One successful example of this from the United States is the Financial Services Information Sharing and Analysis Centre (FS-ISAC), which was formed in 1999 and brings together the public and private sector to enhance cooperation and information sharing to combat cyber and physical threats. It is entirely funded by its membership of over 4,200 organisations which include commercial banks and credit unions of all sizes, brokerage firms, insurance companies, payments processors, and over 30 trade associations representing the majority of the US financial services sector, and works closely with relevant federal, state, and local agencies. It acts as a trusted third party, providing anonymity to allow members to submit threat, vulnerability and incident information in a non-attributable and trusted manner so that information that would normally not be shared, is able to be provided, thereby benefiting the whole of the sector.

20. In this era of tight budgets and rapidly evolving threats, new regulations stipulating particular technologies or practices to address cyber threats are not necessarily required, or indeed appropriate. Instead an outcome based, technology neutral approach should be encouraged, requiring sectors to collaborate and individual organisations to conduct risk assessments, and then put controls in place that are appropriate and commensurate with the identified risk.

21. It is necessary, however, for the government to start taking a more proactive approach to tackling e-crime, rather than the largely reactive structures currently in place. One notable exception is the highly successful Child Exploitation and Online Protection Centre which actively seeks to prevent the sexual abuse of children and catch those involved perpetrating these crimes. The government should consider expanding this pre-emptive policing framework to confront other forms of cyber crime head on.

22. The establishment of the National Crime Agency (NCA) next year provides an opportunity to put such pre-emptive structures in pace. As the government prepares for its formation, it must ensure that NCA's remit, and the boundaries and inter-relationships with other agencies involved with e-rime, are well understood by all. Furthermore, it is imperative for the agencies currently involved in the response to e-crime to continue functioning at their optimum level throughout the transition process to prevent criminals taking advantage of any potential lapses in effectiveness or increased vulnerability.

Whether there are any gaps in the response to e-crime and, if so, how they should be addressed

23. In light of the increasing volume of attacks and rapid pace of change associated with the cyber threat, it is a given that organisations will be in a state of persistent, dynamic, and intelligent threat and disruption. In these circumstances the security dogmas of the past, which rely on an uncoordinated line up of static perimeter defences, can no longer be seen as adequate. Indeed many of the security technologies in common use today across the public and private sector, such as anti-virus software and firewalls, are no longer fit for purpose and offer diminished value in today's world of advanced threats.

24. Security must evolve to a new more agile, risk-based, and contextual paradigm, that takes advantage of the latest advances such as cloud computing and big data analytics, and is able to meet the challenges posed by today's dynamic threats and "hyper-extended" world where information is exchanged in more ways and more places than ever before, and people are using the same devices for their work and personal lives, all enabled by technologies such as smartphones and tablets, cloud computing, and social networking.

25. By doing this, organisations will be able to develop and maintain more flexible security programmes, processes, and technologies that can evolve ahead of—or at least alongside—the threat landscape—and not simply protect themselves against "known bad" threats.

Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use

26. A key barrier hampering the response to e-crime is the fact that organisations that have been targeted by cyber criminals are often reluctant to admit this publicly. This is partly because many organisations fear that

doing so will undermine their corporate reputation and the trust placed in them by their customers and stakeholders. Organisations also perceive that the Data Protection Act and other statutes hamper the sharing of effective actionable intelligence with partners, which as outlined above, can be one of the most effective means of combating cyber crime.

27. RSA recently gained first-hand experience of the importance of both these points, and in particular the importance of transparency and sharing information.

28. On 17 March 2011, RSA publicly disclosed that it had detected a targeted, socially engineered, cyber attack on the company's systems and that certain information related to the RSA SecurID® product had been extracted. RSA immediately developed and published best practices and remediation steps, and proactively reached out to thousands of customers around the world across the public and private sectors to help them implement those steps. Furthermore, RSA worked with the appropriate government agencies and industry bodies in the United States, the United Kingdom and other territories to ensure broad communication of these best practices and remediation steps as well as information about the attack.

29. The attack on RSA has become a valuable lesson that has redoubled the company's commitment to leading industry efforts to increase understanding of today's advanced threats while also collaborating with a broader community of stakeholders to better prepare for and mitigate advanced cyber attacks.

30. To counter these challenges, RSA would urge policy makers to consider legislation providing a safe harbour or similar protections for organisations that voluntarily share sensitive threat information with the government and/or the extant industry information sharing and analysis infrastructure. Such an approach could help improve situational awareness and cyber readiness for many organisations while reducing serious concerns about legal risk. Policy makers should also consider the work being undertaken by the insurance industry to provide innovative means of addressing this issue.

31. In relation to the personal data held by social networking sites, as discussed above it is clear that the preferred method of exploitation for cyber attackers centres on people. With social engineering now the number one avenue of attack, the new security perimeter is in fact the human being.

32. In addition to reinforcing the need for better and increased efforts to share best practice and actionable intelligence on the latest threats and how they can be mitigated, this also demonstrates the need for a shift in corporate culture from the old IT security paradigms towards a more agile, risk-based, and contextual approach that is able to cope with the reality of today's "hyper-extended" world described above.

The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples' online behaviours for related public policy

33. EMC believes consumer education initiatives such as www.getsafeonline.org are crucial to combating e-crime by raising awareness and sharing the latest information on e-crime threat vectors, and how to combat them, as they evolve. EMC has been heavily involved in developing and driving similar initiatives in other countries, notably www.staysafeonline.org, the US equivalent of Get Safe Online, of which EMC was a founding member. The company's global experience of such initiatives suggests their effectiveness is maximised when they are inclusive and involve the broadest possible range of public, private, and third sector partners. EMC would therefore encourage Get Safe Online to enable a broader range of stakeholders beyond the current list of established sponsors and partners to contribute to the initiative, including voluntary groups with established links into the youth sector such as The Prince's Trust. Other private sector partners should also be encouraged to contribute via non-financial means such as by donating staff time and expertise.

34. Finally, the government should consider the tone and positioning of the messages communicated by such educational programmes. Ultimately, the aim should not be to frighten the public or make them think nothing can be done about the cyber threat, and thereby discourage them from enjoying the benefits of today's digital world. Instead the goal should be to convey a simple and positive set of steps that both adults and children can follow to protect themselves, in a same way as was achieved by previous public information campaigns such as the "Green Cross Code" or "Clunk click Every Trip" campaigns to promote road safety. The US

[31] http://www.staysafeonline.org/stop-think-connect/about

Stop.Think.Connect campaign, of which RSA is a founding partner, is a good example of attempting to educate the public on internet security with a clear and engaging set of messages.[32]

August 2012

Written evidence submitted by Get Safe Online [EC 10]

I write to you in my capacity as Chief Executive of Get Safe Online.

As you are probably aware Get Safe Online is part of the Governments supported national major public-private sector initiative to raise awareness of online security. It is aimed at consumers and micro-businesses. It is a not-for-profit organisation and relies on contributions from private and public sector organisations. Current sponsors are: Cabinet Office, BIS, Home Office, Association of Chief Police Officers, The Serious Organised Crime Agency (SOCA), HSBC, Cable & Wireless, PayPal, Gumtree, VeriSign, Symantec, Ofcom and the National Fraud Authority (Action Fraud), Cable and Wireless, Creative Virtual, Trend Micro and Microsoft. It has a board of directors and an active steering group that meets on a bi-monthly basis to set both the strategic and tactical aims and objectives for the initiative on an on-going basis.

The Get Safe Online initiative is largely Internet based. The website at (www.getsafeonline.org) is a one-stop-shop for reliable, independent and easily understood up-to-date information about online safety. It gives home users and small businesses the advice they need to use the Internet safely. It includes information on protecting your PC, yourself and your business as well as advice on topics such as Internet shopping, social networking sites, data theft and identity fraud.

The key messages of the initiative are that online sales and transactions are increasing at an incredible pace. Get Safe Online wants people to be able to continue using the Internet, enjoying the many benefits it has to offer, but also to be aware of the risks and take the steps necessary to protect themselves and their families online. In addition, people are increasingly opting to use the Internet when transacting or interacting with Government and it is important they are online safely and securely.

The Get Safe Online initiative provides a significant contribution to helping computer users and small businesses to take steps to protect themselves, not least because the Get Safe Online name and branding has significant potential and is easy for consumers to remember and therefore access. Government and the private sector will need to continue to work together to ensure that the potential of the Get Safe Online initiative is maximised.

Having outlined the work that Get Safe Online is doing in the area of Internet Security we would welcome the opportunity to give evidence to select committee and to suggest a number of our active partners are also well place to provide significant information to assist you.

Tony Neate
Chief Executive
Get Safe Online

August 2012

Written evidence submitted by Symantec [EC 11]

Given Symantec's position as one of the world's leaders in internet and information security we welcome the opportunity to provide the following information to the Committee in this important inquiry.

Executive Summary

- Today more than ever cyber security incidents have become headline news given the increasingly complex, sophisticated and organised nature of cybercrime which is determined as crime committed using a computer, network, or hardware device.
- Online attacks that were once conducted solely for fame and notoriety are now conducted by organised professionals motivated by economic gain.
- Information continues to be a key target with cyber criminals seeking access to data that can be used to conduct further online attacks or sold as a commodity on the underground economy.
- Cyber criminals tactics continue to evolve by increasing targeting mobile devices and social networks where users may be less aware of cyber security threats and where criminals may be able to avoid detection for as long as possible.
- Recognition by the UK Government that cyber incidents are a tier one level threat is welcomed but given the rapidly changing nature and extent of the threat addressing cyber security must remain a long term overarching public policy objective.

[32] http://www.staysafeonline.org/stop-think-connect/about

— Neither government, industry, law enforcement, individual citizens or Parliamentarian can solve the problem of cyber crime alone.

— Recognition by UK law enforcement of the need to work together and in partnership with industry is a key factor in the effective leadership by the UK in this area.

— But cyber crime is not just a problem for the UK but a global problem that requires a global approach. The involvement of UK law enforcement in international efforts is welcomed and should continue. The rise in data loss incidents has resulted in data protection issues become front page news.

— With personal data a valuable commodity for cyber criminals a sector wider data breach notification requirement should be introduced as part of the current review of the EU data protection legal framework.

— Technology has an important role to play in building and maintaining UK citizens online trust and confidence in the online world. But technology alone is not the answer.

— Raising awareness initiatives that increase understanding of the online threat environment and educate individuals of all agers how to protect their information and identity from the threat of cyber criminals must continue to be supported and funded by both government and industry.

What e-crime is understood to be and how this affects crime recording?

1. To answer this question it is necessary to first define what is meant by e-crime. For Symantec e-crime is included in the term cyber crime defined as any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent, facilitator, or the target of the crime.

2. The broad range of cybercrime can be divided into two categories defined as either a single event or an ongoing series of events. An example of a single event would be where a victim might receive an e-mail containing what claims to be a link to known entity but in reality is a link to a hostile website controlled by a cyber criminal. Once the victim is sent to the hostile website the criminal is in control of a users machine and may take advantage of this control to commit fraud and/or steal individual's information.

3. The second category is an on-going series of events. This can be where there are repeated interactions between the cyber criminal and the victim. For example, the target is contacted in an online chat room by someone who, over time, attempts to establish a relationship. Eventually, by using such use tools as social engineering, the criminal exploits the relationship to commit a crime.

4. When considering what is understood by the term e-crime it may be useful for the Committee to consider the definitions of cybercrime within the Council of Europe Cybercrime Treaty. The Treaty (which the UK government has ratified) is the most comprehensive legal instrument in the fight against cyber crime. In the Treaty cybercrime refers to a number of offences perpetrated using electronic means ranging from criminal activity against data to content and copyright infringement.

5. Overall however it should be remembered that e-crime is not a new phenomenon it is simply traditional crimes conducted using electronic means. For example fraud, harassment and theft has always existed but the new technology is simply the latest tool being used by criminals to conduct their illegal activities. Although clearly depending on what type of crimes are included in the term e-crime this will affect the way in which such crimes are recorded.

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

6. For the last eight years Symantec has produced its Internet Security Threat Report[33] which provides an overview and analysis of worldwide internet threat activity and a review of known vulnerability and trends in areas such as phishing, botnets and spam. The report is based on the most comprehensive sources of internet threat data which is gathered from Symantec's Global Intelligence Network. Information on the key finding of the latest Internet Security Threat Report published in May 2012, can be found at the end of this submission.

7. The findings of the latest report indicate the extent and nature of current cyber threats with Symantec blocking more than 5.5 billion malicious attacks in 2011 which is an increase of more than 81% from the previous year. The number of unique malware identified also increased by 41%. The number of web attacks blocked per day also increased dramatically by 36% as cyber attacks become increasingly complex, sophisticated and targeted.

8. The report shows an increasingly high volumes of malware[34] attacks along with an increase in sophisticated targeted attacks, where the user may not know they are being attacked due to the ability of the attacker to slip under the radar and evade detection, as well as a rise in advanced persistent threats and attacks on the infrastructure of the internet itself. Also identified was an increase in the number of data breaches of individuals and business information with more than 232.4 million identities worldwide exposed overall during

[33] Symantec Internet Security Threat Report 2011 : http://www.symantec.com/threatreport/

[34] Malware is malicious computer code that can be classified into four main threat types: viruses, backdoors, worms and Trojans.

2011. Information remains a key target for cyber criminals who can use personal and business information to conduct other attacks through phishing or social engineering.

9. While the volume and sophistication of cyber attacks globally increased in 2011 the overall level of spam a popular vehicle for conducting cyber crime fell from 85.5% of all email in 2010 to 75.1% in 2011. This reduction is largely seen as due to law enforcement action which shut down Rustock a massive worldwide botnet responsible for sending out large amounts of spam.

10. Cyber criminals are not only continuing to use existing vulnerability but are also increasing in their use of social networks as a propagation vector for attacks. Due to social engineering techniques and the viral nature of social networks it is unfortunately much easier for threats to spread from one person to the next.

11. The growth in viruses and malware attacking mobile devices was also seen with the 2011 report being the first year that mobile malware presented a tangible threat to users. Attacks being seen included malware that sends premium SMS text messages from a users phone. This can earn the cyber criminal $9.99 for each text sent but unfortunately costs the victim dearly when their mobile phone bill arrives. As the take up of mobile phones and tablets continue to rise Symantec expects that cyber criminals will continue to explore ways to attack mobile devices and once they find something effective and money making they will exploit it ruthlessly.

12. Individuals continue to be a key target for cyber criminals according to the findings of the latest Norton Cybercrime Report published on 5 September. One of the world’s largest consumer cybercrime studies the report is based on the findings of a survey of more than 13,000 adults across 24 countries.

13. According to the report there are 556 million victims of cyber crime per year, which is more than the entire population of the European Union. In the UK it s estimated that more than 12.5 million people fell victim to cybercrime in the past 12 months. The cost of cyber crime to the UK was £1.8 billion with an average cost of £144 per cybercrime victim. This means that cybercrime costs UK consumer more than a week’s worth of food for a family of four.

14. The 2012 report showed cyber criminals are targeting users of social networking and mobile devices which is further evidence of how the tactics of cyber criminals are changing based on the popularity of particular technologies and online platforms and networks. It is estimated that two thirds of adults use a mobile device to access the internet. One in five adults globally (21%) has been a victim of either social or mobile cyber crime. In the UK 30% of adults have fallen victim to cybercrime on social networking platforms. Although 63% of adults are accessing social network accounts and 24% access their bank accounts over free or unsecured Wi-Fi connections, around 53% of the adults surveyed were concerned about the security of these Wi-Fi connections.

15. While the 2012 report revealed that internet users are taking basic steps to protect themselves and their personal information, such as deleting suspicious emails and protecting their personal information online other precautions are still not being taken. For example 40% of UK adults don’t use complex passwords or change their passwords frequently. More than a third of adults do not check for the padlock symbol in the browser before entering sensitive personal information such a online banking details.

16. The recognition of the cyber threats as a tier one level threat to the UK in the National Security and Defence Strategy and the subsequent Cyber Security Strategy are seen by Symantec as evidence that policy makers recognise the extent and nature of the threat being faced in the UK. The focus on the economic and social impact of e-crime in the strategy document indicates an understanding of the impact of cyber threats not only to the ongoing resilience and stability of the internet but to the societal and economic stability of the UK. Going forward as the online threat environment continues to evolve there is a need to ensure policy makers up to date on the changing nature and extent of the threat to the UK from cyber crime and that cyber security remain a long term overarching public policy objective.

17. However, addressing cyber threats is not a responsibility of policy makers alone but a responsibility that is shared by all those using the Internet. The nature of the internet and IT technology is such that no single person can be held accountable and we all share a collective responsibility to protect ourselves and our customers whether they are businesses, users or citizens. Public and private sector co-operation and collaboration are a key factor to assisting not only the policy makers but also businesses and individuals to understand, assess and evaluate the level of seriousness of cyber incidents and their level of risk from cyber crime.

The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

18. The UK continues to be seen by Symantec as among the best placed countries in countering cybercrime; particularly in comparison to several other EU Member States. The UK’s Police e-Crime Unit and SOCA’s e-crime task force and the work of CPNI on cyber threats all play an important role in addressing cyber crime issues facing UK businesses, organisation and individuals.

19. A particular element of the effectiveness of UK law enforcement is the strong collaboration with the private sector. Coordination and cooperation between the public and private sector on addressing the spread of

cyber crime are an important component to a cyber security strategy not only in the UK but also globally. The UK's understanding that it is the private sector that has most knowledge about cyber threats and the need for law enforcement and industry to work together in collaboration, where appropriate, should be seen as a key success factor of the UK approach. However, it is also suggested that providing more training and resources to UK police , particularly at a local and regional level to fight cyber crime would be welcomed.

20. Given that the proposed organisational changes have not been implemented yet, it remains to be seen how the establishment of the National Crime Agency (NCA) will affect enforcement activities in this area. The proposals outlined by the Home Office in June 2011 point towards a continued focus on cyber crime as there currently is within SOCA and the Police e-Crime Unit. The creation of a National Cyber Crime Unit that it is understood will sit within the NCA is also welcomed as by Symantec. This step forward points the way forward for law enforcement capabilities already in place to be enhanced and bolstered going forward. Before the NCA is in place the emphasis in the Home Office document s on the importance of the continued cooperation between SOCA and the Police e-Crime Unit before the NCA is established is supported.

21. However, it should also be remembered that cyber crime is not just a local, regional or even national problem for the UK. Cyber crime is a global problem that requires a global approach particularly as threats and attacks can travel around the world at the click of a button. It is suggested that a move towards a more European wide approach by law enforcement to cybercrime issues could support and enhance the effectiveness of current UK efforts. Symantec has welcomed the recent announcement of the establishment of a Europol Cybercrime Centre. It is hoped that this initiative will continue to develop cooperation and coordination by law enforcement and that UK law enforcement will play a key role in supporting the Centre's activities.

22. In terms of legislative capabilities the UK's legal framework for addressing cyber crime is supported by Symantec. The Computer Misuse Act is a key legislative tool and provides the capability for prosecutions related to cyber crime offences. However, as explained above new forms of cyber crime emerge as new technologies develop. Given the rise in online threats since the Computer Misuse Act was last amended in 2007 it is suggested that the Committee should considered whether there are aspects of cyber crime seen today that remain unaddressed within UK's legislation. For example while unauthorised access to a computer is criminalised under the CMA the actual theft of confidential information is not specifically addressed. In light of the significant number of UK citizens being affected by identity related online fraud it is suggested that a discussion is held on whether this offence should be specifically addressed within UK law. Also given the take up and use of cloud computing by both businesses and citizens increases a legislative gap currently exists in both UK and EU law given that the use and also misuse of computing resources delivered via the cloud without right is currently not covered within either UK or EU law. These offences are suggested as areas that the Committee could considered to ensure that the UK's legislative capabilities are sufficient to address current and possible future online criminal activity.

Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use

23. As the Committee's question highlights the findings of Symantec's latest internet security threat report shows that information continues to be a key target for cyber criminals as well as a rise in the use of social networks by cyber criminals to conduct attacks. With hundreds of millions of people on social networking sites it is inevitable that online criminals would look to attack users there. However according to Symantec's findings more than half of all attacks identified on social networking Web sites were related to malware hosted on compromised blogs or communication sites rather than the theft of information from social networking sites. It appears that a key threat from social networking is where a hyperlink for a compromised website is shared to a large number of users on a social network. Users then click on the link and are sent to the website where malware, which may include threats such as key loggers that seek access to personal information such as passwords, can then attack their machines.

24. Given the rise in data breaches and the threats seen to personal information Symantec has welcomed the European Commission review of the current European data protection legal framework in place in Europe since 1995 which is proposing the introduction of a sector wide data breach notification requirement The review of the current Data Protection Directive (95/46) from which the UK Data Protection Act 1998 derives, is an opportunity to ensure the legal framework, first introduced in 1995 is appropriate and relevant today; particularly in an era where information has become the digital currency for users but, unfortunately, also a focus for e-crime.

25. Gaining and maintaining the trust and confidence of individuals that their information is protected and secured given the level of cybercrime being seen is a challenge that must be faced and addressed by organisations. Introducing a requirement to notify if data has been lost or stolen in the legal framework not only ensures data is fully protected throughout its lifecycle but also that users are informed if a serious incident occurs that may impact them, thus creating a sense of empowerment and individuals' confidence in taking action if they want or need to. However, any breach requirements introduced needs to be appropriate and non burdensome to either organisations or citizens.

26. While ensuring the data protection legal framework in Europe is appropriate and relevant to the way information is being processed, accessed, shared and managed online, there is also a responsibly of individual users to ensure that they protect their information particularly when sharing personal information online.

27. The computer security industry has an important role to play in developing technological tools and solutions that are appropriate to deal with cyber threats and can help individuals to protect their identifies and information online. Symantec will continue to develop and offer solutions that enable users to put in place appropriate measures to protect their systems, networks and information. However it should be recognised that software companies cannot and should not be held responsible for what they do not effectively controls such as how a users may install, configure, use and update (or perhaps even chose not to update) security software. It is also difficult to see how a technology provider would measure the responsibly of the consumer in the way it has selected, installed, configured and users the software when ascertaining liability.

28. Factors that would need to be considered in measuring and determining possible liability would include whether the software being used by an individual user is fitness for the purpose it is being used. For example is the software being used in line with its intended purpose. Also whether the software being used is up to date and properly maintained by the user. For example a user may have decided to turn off the automatic software updates provided by the provider when the user configured the software. This is a decision that the provider of the software will not be aware of nevertheless this action could result in the user being left unprotected whilst online and suffer a cyber incident. In such a scenario the individual user may suffer cyber attack not because the software failed but because of a decision made by the user.

29. If such an approach was taken for it to be workable it is suggested that software vendors would need to be able to gain the necessary control over the way that users are using their technology. This could include the ability to monitor and control the behaviour and actions of people for example to ensure that the software, or tool, is being used for only the purpose for which it was supplied or sold. Moves in such a direction would not only raise political, privacy and legal questions but it is not clear whether such a evolution in the way in which technology interacts with users is a journey that users would be willing to embark on and potentially cover the costs of.

30. An approach where the liability burden is placed on the provider of software products alone could lead to a situation where companies would not be prepared to take liability for their products unless they can assume a level of control over the way it is being used in order to avoid or limit liability. This could lead providers to using more privacy invasive technological to provide the ability to monitor and control the behaviour and actions of users for example to ensure that the software is being used for only the purpose for which it was supplied or sold.

31. An approach along these lines could not only impact the control users have on their PC's but could also stifle technological innovation and competition in the marketplace by promoting particular business models. A move towards more closed platforms or a situation where one dominant technology provider could dictate what can, or cannot, be installed on its system due to liability concerns may limit consumer choices to only sites or online content that are approved by PC providers based on a level of risk.

32. Moves towards liability in this area could not only raise political and legal questions but it is not clear whether such a evolution in the way in which technology is provided and interacts with users is a journey that users would be willing to embark on and potentially cover the costs of its development and implementation.

33. As the online threat environment continues to evolve and cyber criminals tactics adapt and change it is only right that we continue to consider options for addressing current as well as emerging issues. However in light of the rapid speed in which cyber threats and attacks evolve it is important that legislation and law makers should not try to run behind technology but rather support the market to develop the appropriate tools and solutions to current and future online threats. Also it is also important that users continue to be educated about online threats and understand the value of their personal data and the importance of having protection measures in place that are appropriate to their online activities.

The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples' online behaviours for related public policy

34. Having appropriate technological solutions and tools in place can support citizens to have the confidence that their activities and information and identity online are being protected. However, Symantec believes that technology alone is not enough to address the online security challenges we all face today. An effective cyber security approach is one that combines appropriate technology, the development of policies, procedures particularly for reporting, responding and recording cyber incidents and raising awareness initiatives to ensure people have the necessary skills and knowledge to protect themselves from cyber criminals.

35. Symantec continues to be a supporter of initiatives around the world that promote awareness of internet security and safety issues to different online users from children to silver surfers. In the UK Symantec has been a long term supporter of Get Safe Online the government-industry campaign aimed at raising greater awareness amongst citizens and small businesses of the importance of online security. We are also members of the UK Council for Child Online Safety which is another example of how industry and government are working in partnership to increase understanding of online safety by both children and parents.

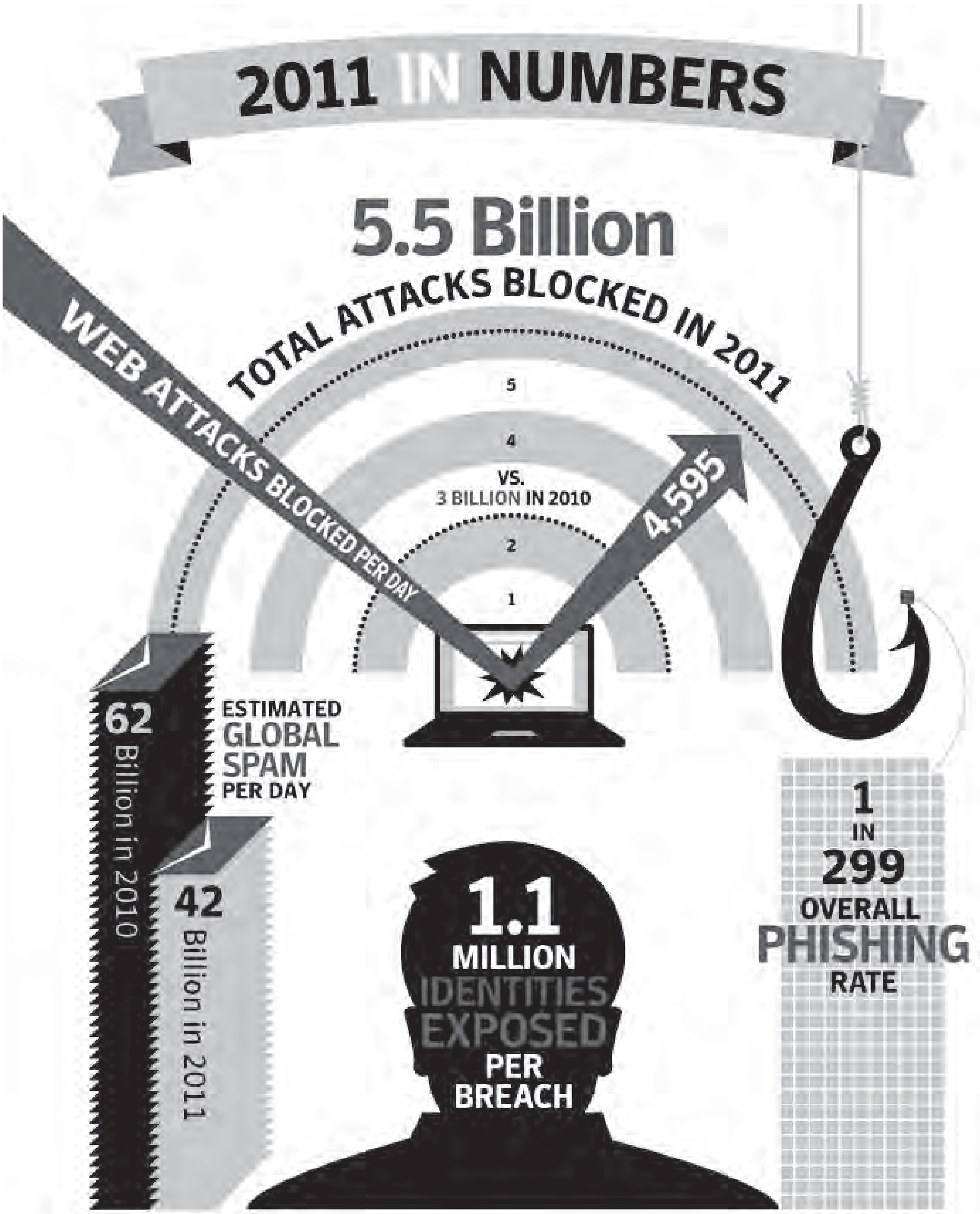
36. At a time when public and private sector organisations continue to look to online platforms and networks to interact and provide goods and services directly to citizens, it is important that internet security and safety remains on the public policy agenda. Initiative and activities that can raise awareness of the online threat environment and the importance of online security and safety have a key role to play not only in protecting individuals information online but also creating greater trust and confidence of internet technology. This will remain important if we are to ensure UK citizens can gain from the full opportunity and advantages offered by the internet and have confidence to enjoy the connected world safely and securely.

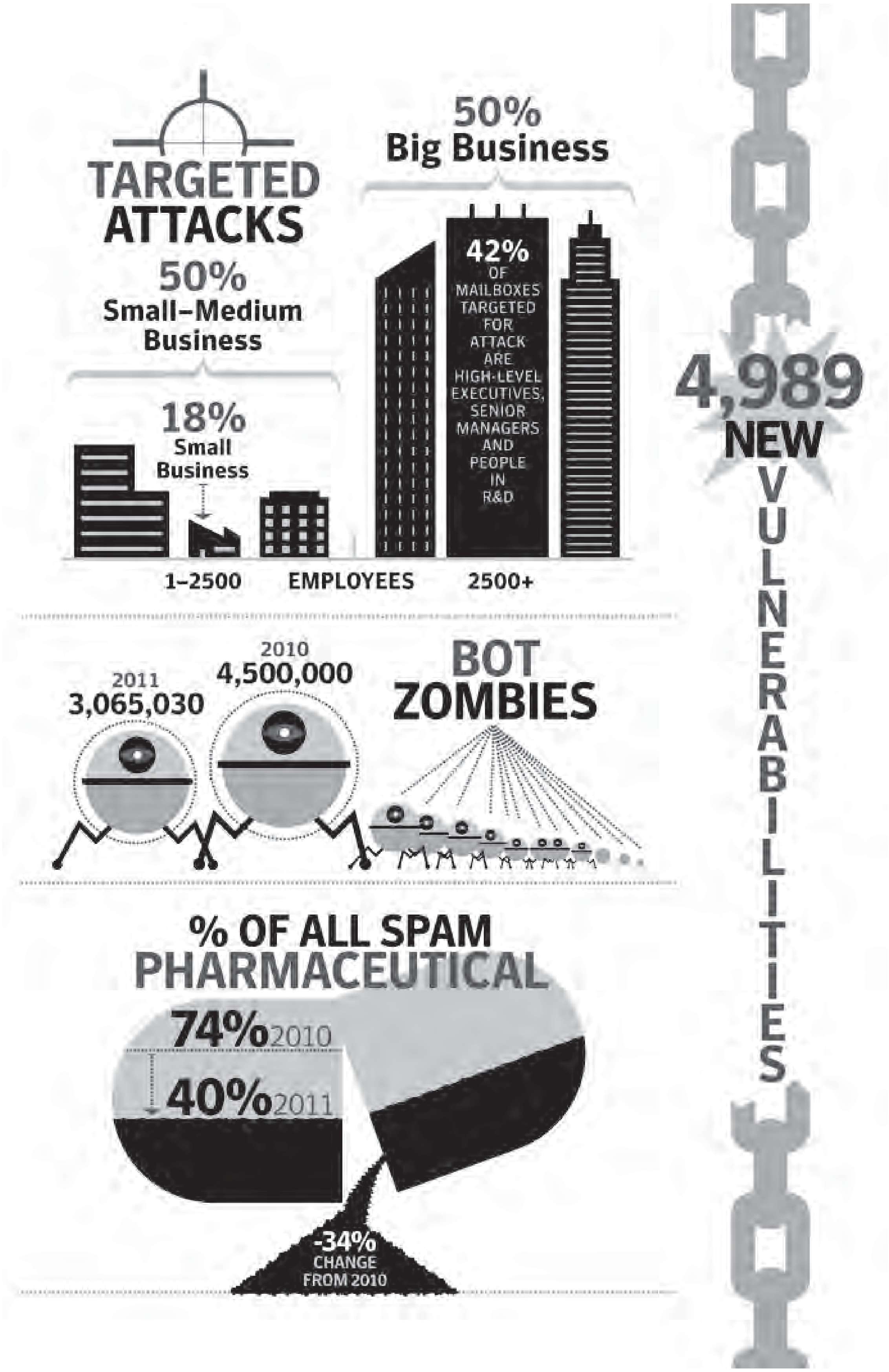
37. As mentioned earlier in this submission addressing cyber crime threat facing the UK is not something that industry, government, individuals or law enforcement can do alone. Users also have a responsibility to protect themselves by installing and using available internet products and tools effectively to ensure they remain secure. Education on online security and activities that raise awareness will continue to be vital to ensuring users are aware of not only the constantly evolving online threat environment but also what they can do to be safe and secure online.

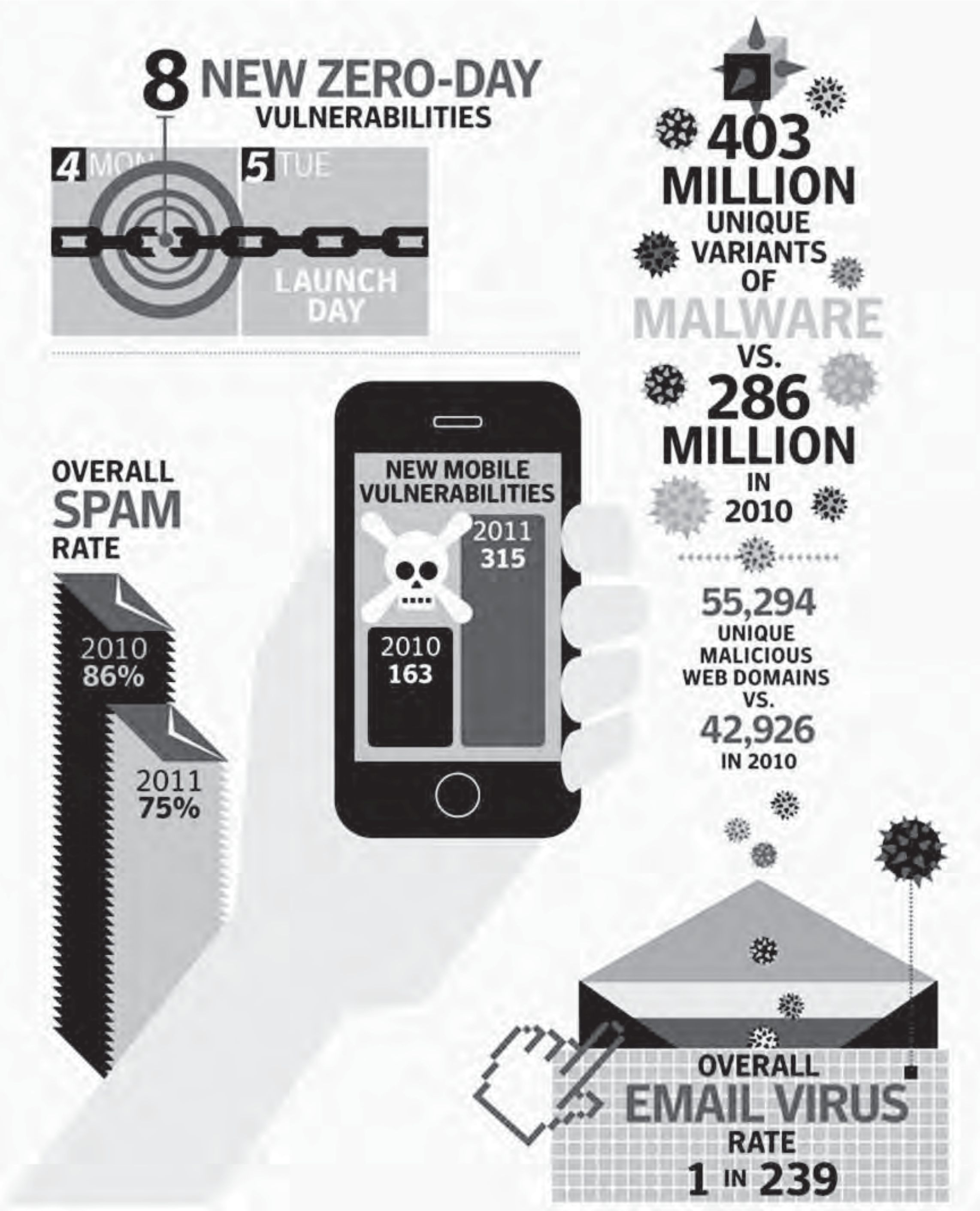
38. While the current economic climate presents many resources challenges, it is important to continue to invest in ensuring individuals are aware of cyber security issues if the full social and economic opportunities and benefits offered by online networks and platforms are to be fully realised.

Symantec is a world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. Further information can be found at www.symantec.com. Symantec appreciates this opportunity to submit comments to the House of Commons Home Affairs Select Committee.

October 2012


2011 IN NUMBERS
5.5 Billion
TOTAL ATTACKS BLOCKED IN 2011
5
4
VS.
3 BILLION IN 2010
2
1
WEB ATTACKS BLOCKED PER DAY
4,595
62
Billion in 2010
ESTIMATED
GLOBAL
SPAM
PER DAY
42
Billion in 2011
1.1
MILLION
IDENTITIES
EXPOSED
PER
BREACH
1
IN
299
OVERALL
PHISHING
RATE


TARGETED
ATTACKS
50%
Small–Medium
Business
18%
Small
Business
50%
Big Business
42%
OF
MAILBOXES
TARGETED
FOR
ATTACK
ARE
HIGH-LEVEL
EXECUTIVES,
SENIOR
MANAGERS
AND
PEOPLE
IN
R&D
1–2500
EMPLOYEES
2500+
2011
3,065,030
2010
4,500,000
BOT
ZOMBIES
% OF ALL SPAM
PHARMACEUTICAL
74%2010
40%2011
-34%
CHANGE
FROM 2010
4,989
NEW
VULNERABILITIES



Joint written evidence submitted by the National Trading Standards Board, the National Trading Standards eCrime Centre, the Association of Chief Trading Standards Officers and the Trading Standards Institute [EC 12]

This response has been submitted to the Home Affairs Committee eCrime Inquiry by the National Trading Standards Board (NTSB), the National Trading Standards eCrime Centre (NTSeCC), the Association of Chief Trading Standards Officers (ACTSO) and the Trading Standards Institute (TSI) and was produced by Mike Andrews (NTSeCC) and Paul Thompson (Warrington & Halton Trading Standards).

Introduction

1. Local Authority Trading Standards Services (LATSS) enforce a wide range of consumer protection legislation across the UK. In the past this has been focussed on the traditional "high street" where a physical premise could be visited and problems could be addressed in a much more tangible way. However, the internet

has brought a whole new market place to consumers in the UK which has led to Trading Standards having to adopt new and innovative approaches to ensuring adequate protection for consumers carrying out their transactions online. As more and more consumers and businesses now routinely use technology (be that internet, e-mail or mobile/smart phones), Trading Standards faces further challenges in ensuring internet scams are properly tackled.

2. Trading Standards has a vital role to play in an overall strategy of e-crime enforcement. The security and integrity of the internet is key to the future economic success of the UK. Consumers need to feel they are adequately protected when carrying out their business online and equally, businesses need to be confident that rogue traders operating online are robustly tackled. Trading Standards takes the leading role in ensuring both these priorities are met and welcomes the opportunity to submit written evidence in relation to this inquiry.

What e-crime is understood to be and how this affects crime recording

3. The terms e-crime and cyber crime are often used interchangeably but are, broadly speaking, one and the same. The ACPO definition of e-crime is; "The use of networked computers or internet technology to commit or facilitate the commission of crime". This is a perfectly reasonable definition but can cover a wide range of offending and there is often a lack of clarity as to the types of criminality that fall within that definition. Indeed, there is (in law) no such crime as an "e-crime". This in itself can lead to problems in the effective reporting and recording of e-crime, as outlined later in this section.

4. The UK Cyber Security Strategy and previous discussions on the subject of e-crime have tended to focus, quite reasonably, on the higher level criminality such as hacking, Distributed Denial of Service (DDoS) attacks, cyber terrorism and large scale data/identity theft. However, in relation to consumer and business impact, there are a number of areas that whilst individually may be perceived as low level criminality, they can often have a disproportionate effect on the individuals concerned. These are often crimes that are not specifically dependant on technology to facilitate the crime, as would be the case for DDoS for example. However, the proliferation of technology has made the commission of the offences far easier and allowed the offenders to target a much wider audience than they would previously been able to using "traditional" methods. For example, the sale of counterfeit goods or websites set up to encourage consumers (and businesses) to part with their money without the product or service ultimately being provided. In terms of the National Intelligence Model (NIM) much of this would appear at first glance to be Level 1 criminality. However, when the scale of offending is assessed it can quite often become apparent that this in fact Level 2 (and in some cases Level 3) criminality.

5. In relation to the recording of e-crime, in practice the ACPO definition and most other definitions fail to provide for the successful recording of all instances of e-crime. This is primarily because the e-crime element is often a sub-element of the actual mischief of the crime. For example, a trader using a website to commit some sort of advance fee fraud might be classified as a fraud offence, when the principal mechanism to facilitate the crime is the internet. Furthermore, there is a proliferation of mechanisms by which consumers and businesses can report/record instances of e-crime. This in itself leads to an inaccurate picture as to the true scale of e-crime (see paragraph 16).

The extent and nature of the threats on which e-crime policy is based and how well they are understood by policy makers

6. Broadly speaking, Central Government would appear to have a good understanding of the higher level threats posed by e-crime. However, there is probably less of an understanding of the threats posed directly to consumers and businesses when going about their normal day to day business, for example; websites offering fake job opportunities, companies offering to provide a service with up front fees that then fail to deliver the service (advance fee fraud) and websites selling counterfeit, dangerous and/or illicit products. The Federation of Small Businesses believes e-crime is having a serious detrimental impact on their economic success.

7. The creation of the National Trading Standards eCrime Centre (NTSeCC) (see paragraph 15) has gone some way to begin to address this issue. However, there still remains a lack of recognition amongst policy makers as to how that may fit within an overall approach to tackling e-crime. The priority thus far, as one would expect, has been tackling the high level threats to national security. From a local policing perspective, the policy has tended towards tackling the spread of child pornography. As a consequence, the very real threat from general scams that are targeted at UK consumers has tended to be poorly understood. Anecdotal evidence suggests that, what appears to be relatively low-level criminality can have a disproportionate impact on those individuals affected. To someone on a relatively low income, losing £100 through some form of internet scam could be extremely detrimental to their well-being. As an economy we are increasingly reliant on e-commerce so policy makers need to fully understand the impact of this type of criminality and the detrimental effect it has in creating a trusted online environment.

8. As outlined above, policies are often considered and devised based upon serious and organised criminality (eg Home Office Guidance and Implementation of RIPA Notice for use with Facebook, Charles Miller April 2010—which focused primarily on SOCA/Police access to Facebook). Much more detailed consideration needs to be given to the impact e-crime has at Level 1, particularly from a Trading Standards perspective as this often forms part of much wider Level 2 and Level 3 criminality. If one considers the Home Office guidance referred to above, the process was considered and is only relevant for SOCA/Police, as a result the disclosure

process can only be accessed by SOCA/Police Single Points of Contact (SPoC). Even then the disclosure process does not go far enough to assist with localised law enforcement issues faced by Trading Standards.

9. Purely from a Trading Standards view point current legislation in relation to e-crime is often a case of applying square pegs to round holes. For example, obtaining disclosure from a hosting company should ordinarily be a straight forward Data Protection Act request. However, quite frequently hosting companies will refuse on the grounds the information is telecommunications data. Another example would include obtaining disclosure from social networking sites, for example Facebook, as referred to previously. The inability of regional law enforcement officers to obtain data pertinent to a Facebook account, whereby the account holder involved in criminality has closed privacy settings, is in effect giving the criminal fraternity an open passport to trade illegally.

10. These examples highlight the gaps between policy makers and law enforcement agencies which have a duty to enforce e-crime at Level 1. Unfortunately, the difficulties posed by these gaps often result in little or no action being taken to identify and apprehend individuals involved in e-crime, let alone anyone connected to organised gangs. Furthermore, this fundamental lack of enforcement ability at Level 1 fails to provide the information necessary to deliver the intelligence building blocks which are required to carry out successful enforcement at Level 2 and Level 3.

The effectiveness of current law enforcement and legislative capabilities, including local and regional capabilities and the potential impacts of proposed organisational change

11. Recent organisational changes would appear to have been successful in having an impact in tackling the serious, national e-crime threats that we are faced with. The creation of PCeU, SOCA Cyber and others is certainly a step in the right direction. Clearly, it remains to be seen what impact the creation of the National Crime Agency (and in turn the National Cyber Crime Unit) will have in tackling e-crime.

12. In respect of Trading Standards, changes to consumer protection enforcement that have led to the creation of NTSeCC are a welcome move in recognising the importance of tackling all forms of e-crime and not just those at a high or serious organised crime level. However, there still remain some fundamental issues which need to be tackled:

(a) Resource issues/training: hindering the appropriate investigation into e-crime, impacting on appropriately trained staff and the ability to keep up to date with technology and the ever changing techniques of the e-criminal.

(b) Localised political agendas: the level of e-crime enforcement within Trading Standards at a local level is very much at the discretion of local political priorities and their views of the requirements of the communities they represent. For example, a rural local authority may have more interest in animal feed enforcement than investigating intellectual property crime on the internet. This factor has even more impact given the public sector cuts in recent times which have forced local authorities to review their priorities which inevitably has removed resource from enforcement functions.

(c) Central Government: the continued need for policy development to prioritise local/regional law enforcement. This often results in the tools (resource & legislation) not being provided for law enforcement officers to deal with e-crime effectively. The recent changes to RIPA are a point in case whereby LATSS staff will now have to seek magistrates' approval in order to gain access to subscriber data. Although it is recognised why policy makers sought to restrict isolated disproportionate use of RIPA, for Trading Standards enforcement, this appears to be a wholly disproportionate change that will severely impact on the ability of local officers to tackle e-crime.

13. With reference to resources and training, NTSeCC is about the undertake a programme of work to ensure Trading Standards enforcement staff are suitably trained to carry out e-crime investigations at a local level. This will include improving their knowledge of open source research, online investigation techniques and the capture of digital evidence. Allied to that is a programme of equipment procurement to ensure local staff have the correct tools (both software and hardware) to help them further their investigations.

Whether there are any gaps in the response to e-crime and, if so, how they should be addressed

14. The Consumer Landscape Review, commissioned by the Government in 2011, set out a vision to, amongst other things, improve and simplify the way in which consumer protection legislation was enforced locally, regionally and nationally. Traditionally, the majority of this work was split between the Office of Fair Trading (OFT) and individual LATSS. With the differing remits (and geographical boundaries) of the two bodies, this often led to "enforcement gaps", particularly when dealing with cross-region and national issues. In recognition of this, the National Trading Standards Board (NTSB) was formed to oversee the transition of responsibilities from the OFT to LATSS, with particular emphasis on putting in place an infrastructure to tackle cross-region and national issues and/or cases of a particularly complex nature (Level 2 and Level 3 criminality).

15. As part of this process, the provision of e-crime enforcement in relation to scams and rip-offs directed at consumers and businesses was indentified as a key priority. Whilst there are a number of officers in individual

LATSS who take an active role in e-crime enforcement, there was no coherent approach to tackle a problem which, by its very nature, is a cross-region issue. It was also recognised that e-crime enforcement is a specialised area, requiring specific expertise and skills. Furthermore, for reasons already identified, this area of e-crime has not always been seen as a priority by other enforcement agencies. As a result, the new NTSeCC has been formed to tackle the problem of internet scams directed at consumers and businesses.

16. Consumers and business are faced with a bewildering array of options when reporting e-crime. The local police force, LATSS, Citizens Advice, Crimestoppers and Action Fraud are just some of the reporting mechanisms available. As a result, it is sometimes difficult to build up a complete and accurate picture of the current and emerging threats faced. NTSeCC has recognised this as a key issue and therefore the collection and analysis of intelligence in relation to e-crime is core to its business. This will allow us to monitor current and future trends so we can direct our limited resources in a way that is likely to have the most impact. However, it is felt that greater clarity needs to be provided as to where to report instances of e-crime. If this is through a central point (for example Action Fraud) then this needs to be backed up by clear, simple processes that allow for the rapid dissemination of reports to the appropriate agencies for action (ie NTSeCC, LATSS etc).

Options for addressing key emerging issues that will affect the public such as liability over personal computer security, personal data held by social networking sites and its vulnerability to criminal use

17. NTSeCC is currently undertaking a National Strategic Assessment with a view to identifying emerging threats faced by consumers that are specific to areas that Trading Standards has a duty to enforce. However, as part of the wider Trading Standards role, we have a duty in terms of safeguarding vulnerable people. In line with this, Trading Standards would look to support any activities through its links with Citizens Advice and their wider Consumer Empowerment Projects.

The effectiveness of current initiatives to promote awareness of using the internet safely and the implications of peoples' online behaviours for related public policy

18. There are a number of initiatives aimed at raising awareness such as Know The Net, Get Safe Online and Action Fraud. Whilst these are worthy attempts to give the public a greater awareness, there doesn't seem to be a coherent response to tackling this issue. Frequently consumers and businesses put themselves in positions whereby they are easy prey for online criminals. This is often as a result of being poorly educated in the potential dangers of the internet and being unaware of the personal and financial risks they undertake whilst using the internet/computers.

19. One could question whether this should be the sole responsibility of Government or whether the industry (ISPs, search engines etc) should take on a more pro-active role in educating their customers to some of the pitfalls of using and trading on the internet. Whilst we recognise that steps are already being taken by some parts of the industry, there are elements that seem to "turn a blind eye" to both their moral (and in some cases legal) responsibilities.

November 2012

Written evidence submitted by Professor Peter Sommer [EC 14]

1. I am currently a Visiting Professor at de Montfort University and a Visiting Reader at the Open University. For 17 years I was first a Visiting Research Fellow and then a Visiting Professor at the London School of Economics. I have acted as an expert witness in many trials involving complex computer evidence; many of these would probably be regarded as E-Crime. They include: global hacking, terrorism, "phishing", software piracy. But my instructions have also included criminal matters where digital evidence was crucial although the substantive crimes, including murder, large scale illegal immigration, art fraud, state corruption, money laundering, insurance frauds, theft of gold bullion and paedophilia which would probably not be classified as E-Crime.

2. I have provided advice for the UK's National High Tech Crime Training Centre, was the external evaluator and then external examiner for the MSc in Computer Forensics at the Defence Academy at Shrivenham which is widely used for police training and while it existed I was the Joint Lead Assessor for the digital element in the Home Office-backed Council for the Registration of Forensic Practitioners. I currently advise the Forensic Science Regulator on matters of digital evidence.

3. As an academic I have had a very long-standing interest in the issues of the definitions and statistics of computer-related or "cyber" incidents. In March 2009 I carried out a literature review, including statistics, of Internet crime for the National Audit Office as a contribution to a value-for-money review of Government initiatives in reducing the impact of such crimes.

4. From time to time I have been asked to contribute to a variety of government-sponsored inquiries into the policing of e-crime, starting with Project Trawler in 1999 which lead up to the formation of the National High Tech Crime Unit.

5. My practical work as an expert witness has brought me into frequent and direct contact with successive specialist police units, starting with the original Metropolitan Police Computer Crime Unit.

6. In February this year the House of Commons Science and Technology Select Committee published its report *Malware and Cyber crime* (HC1537) for which I provided both written and oral evidence. Both appear in their printed report. There is some slight overlap with the concerns of your Committee's current inquiry and this is reflected in my submission to you, though of course the two Committees proceed on different bases.

7. I attach a CV.[35]

Definitions of E-crime

8. There is no generally-agreed definition of E-crime and this lack directly impacts assessments of extent. We can illustrate the diversity of definitions. The Council of Europe CyberCrime Convention,[36] also known as the Treaty of Budapest, covers in Articles 2–6 as "substantive offences": "illegal access", "illegal interception", "data interference", "system interference", and "misuse of devices". It adds as "computer-related offences", articles 7 and 8, "computer-related forgery" and "computer-related fraud". It further adds, articles 9 and 10, "offences related to child pornography" and "offences related to infringements of copyright and related rights". Articles 4 and 5 more-or-less correspond to s 3 of the UK Computer Misuse Act, 1990: "Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc."

9. If we now turn to a report produced in February 2011 by the BAE subsidiary Detica in partnership with the Cabinet Office's Office of Cybersecurity and Information Assurance (OCSIA), *The Cost of Cyber Crime,*[37] this covers: "identity theft and online scams affecting UK citizens; IP theft, industrial espionage and extortion targeted at UK businesses; and fiscal fraud committed against the Government". "Industrial espionage" is not a criminal offence in the UK[38] and the report excludes any direct reference to malware or to child pornography.

10. A recent paper by academics at Cambridge and Cardiff Universities *Measuring the Cost of Cybercrime*[39] has the great virtue that it carefully discusses the various elements that might go into "cybercrime" and estimates of associated loss. At the very least the reader can see the workings and assess whether to accept their particular decisions. A similar earlier and slightly less thorough exercise was carried out by the Oxford Internet Institute in 2010: *Mapping and measuring Cybercrime.*[40]

11. The *ACPO E-Crime Strategy*[41] dated August 2009 uses a much simpler definition: "The use of networked computers or Internet technology to commit or facilitate the commission of crime". This definition appears to exclude, for example, the use of computers to carry out frauds which don't involve networks, the acquisition of illegal material such as child or extreme pornography and the deployment of techniques to generate forged documents.

12. The previous ACPO Strategy, dated January 2005 and signed off by Trevor Pearce, then Acting Director General of the National Crime Squad and now Director Designate of Operations at the National Crime Agency (NCA), referred to "For the investigation of Computer-enabled Criminality and Digital Evidence"[42] and did not limit itself to "networked computers or Internet technology".

13. It needs to be recognised that by 2011 PC ownership was 77% of the population and household internet take-up was 78%.[43] When the term "computer crime" first came into popular usage in the early 1970s the proportion of the population that had access to computers was tiny. For that reason, right through to the end of the last century it was possible to see computer/cyber/e-crime as distinct purely in terms of the demographics of potential offenders. But today large numbers of crimes are likely to have a "computer" element simply because for most of the population distinctions between their "non-virtual" and "cyber" selves are increasingly difficult to make.

14. The computer and the network may not be central to a crime or its investigation but the role of some form of digital evidence may be crucial.

15. A question for the Committee, therefore, is whether the current ACPO definition of E-Crime fully addresses the range of policy issues facing police investigatory capability.

Impact on Crime Reporting

16. Most official forms of crime recording in the UK are on the basis of specific offences prosecuted. But in relation to "E-crime" there are particular difficulties as a result of policies of the Crown Prosecution Service.

[35] Not printed.

[36] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. It dates from 2001 and came into force in 2004 and was ratified by the UK in 2011.

[37] http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

[38] http://www.justice.gov.uk/lawcommission/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_Trade_Secrets_Consultation.pdf

[39] http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

[40] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694107

[41] http://www.met.police.uk/pceu/documents/ACPOecrimestrategy.pdf

[42] I have been unable to discover a current online source for this, but retain my own copy

[43] Ofcom http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr11/UK_CMR_2011_FINAL.pdf

It sees the 1990 Computer Misuse Act as designed to fill in gaps in other forms of legislation[44] and in framing charges will concentrate on what it sees as the substantive offence rather than a *modus operandi*. Thus, if some-one infiltrates a program to monitor the keystrokes on a computer and then subsequently uses the passwords thereby obtained to access a computer from which to carry out a fraudulent transaction, the offence will probably be recorded as a breach of the Fraud Act 2006, despite the fact that both s 3 and s 1 Computer Misuse Act offences took place. A phishing attack would probably also be charged as fraud or money laundering, a Distributed Denial of Service attack (which also tends to involve offences under s 3 Computer Misuse Act when computers are remotely taken over by "back doors" or "Trojans") would probably be charged as an extortion as this is the most common way in which criminals can make money. A botnet is simply a more extensive form of Distributed Denial of Service attack. In every year since the Computer Misuse Act came into force, prosecutions have seldom exceeded 100 per year.

17. From a broader policy perspective many criminal activities can be classified in several different ways—as the "substantive" offence such as fraud, sexual exploitation of children or extortion—or as a "computer crime" (involving computers to some degree) or as an e-crime (on the current ACPO definition as involving networked computers).

Impact on Policy Formation

18. The main justification for collecting statistics and arguing about categorisation is to see that resources are available to meet the needs of law enforcement, a matter which I consider below.

Gaps in Legislation

19. There are no significant gaps in terms of substantive law, as a combination of existing conventional criminal offences, principally the Fraud Act 2006, and the deployment of the Computer Misuse Act meet most likely eventualities. There are however problems with the law covering investigators, which consists of a hotch-potch of powers, the product of historical evolution. Seizure and subsequent examination of computer hard-disks and other physical data media depend mostly on the Police and Criminal Evidence Act, 1984. Communications data is covered by the Regulation of Investigatory Powers Act, 2000 and subsequent laws and orders about data retention, currently the subject of the Draft Data Communications Bill. Interception evidence is, under RIPA, inadmissible and can only be used for intelligence purposes. The law covering access by the police to suspect computers is particularly complex and I attach a copy of my article *Police Powers to Hack* which is in *Computer and Telecommunications Law Review* (2012 CTLR, Issue 6 pp 13–19).[45] There, and also in my evidence to the Joint Committee Draft Data Communications Bill, I suggest that a more radical review of police powers, including the circumstances in which warrants are issued, is required in order to achieve an appropriate balance between providing the police with adequate investigatory powers and ensuring that the public are not subject to unnecessary intrusion.

20. Interception evidence, currently excluded by s 17 RIPA, 2000, will need to be admitted in the same way as all other forms of technical evidence and the distinctions between "communications data" and "content" are now almost impossible to make within the technical protocols used on the Internet.

21. The Committee also ought to consider the position of the means by which evidence is obtained from cloud computing services, the vast majority of which are not based in the UK either jurisdictionally or physically. There are many forms of cloud computing, from consumer-orientated services like Google, Facebook, Drpbox, Twitter and web-based email, to business facilities in which companies substantially reduce their own local computing resources and pass their processing and storage requirements to large international entities.

22. Although there are a number of legal procedures and Mutual Legal Assistance Treaties which give the UK courts the ability eventually to obtain evidence from the cloud, they are lengthy and expensive. Swifter results can be obtained by seeking the co-operation of cloud companies, but the UK government seems slow to realise that the cloud companies will strongly prefer adherence to international legal norms of recognition of privacy rights, transparency, strict application of necessity and proportionality tests, and proper judicial process. In that connection, UK use of law enforcement-issued production orders and permission to intercept in the hands of a politician, is significant handicap.

Issues in Investigation and Law Enforcement

23. Apart from the matter of investigatory powers, the very wide range of circumstances in which digital evidence may play a part creates significant difficulties for determining a police response. A criminal event may be local, national or international; it may be semi-opportunistic or highly organised; it may or may not, be linked to other forms of organised crime; its primary focus might be fraud involving banking and financial services, or retail fraud, or the sexual abuse of children, or the theft of copyright materials, or something else entirely. And the digital evidence may be central to a trial or simply peripheral but essential.

[44] Statements frequently made by CPS officials in public and private

[45] Not printed.

24. It is not enough to think in terms solely of specialist units. *Every detective needs to know the basics of digital evidence—where it is likely to be located, how it can be safely collected and preserved without being contaminated in the process, and the core techniques that are used in analysis*. The front-line detective needs to be able to interact and work with forensic technicians. Because of the ever-changing nature of computer hardware and software, and the rapid development of new criminal methods, basic training for all detectives cannot be a one-off exercise but requires relatively frequent refreshment.

25. In effect the *police response needs to be tiered*—a level of knowledge for all, higher levels of skills for detectives within particular specialisations such as child protection, fraud, terrorism. And a single elite leadership unit to tackle the most complex and innovatory crimes and also provide research, advice and training for the rest of the law enforcement community.

26. The first attempt at setting up such a unit was the National High Tech Crime Unit (NHTCU) and which disappeared when the National Crime Squad was dissolved and the Serious Organised Crime Agency (SOCA) created. NHCTU staff were then absorbed in to "SOCA e-Crime", now "SOCA Cyber". But SOCA was separate from UK policing and the leadership role was lost until PCEU was set up from within the Metropolitan Police Service. It is to be hoped that with the development of NCCU within NCA does not repeat the same mistake—the unit must have a solid clearly articulated on-going relationship with the rest of UK law enforcement.

27. Thought must also be given to how digital forensic expertise is made available. The expertise has to extend to assisting in making decisions about what potential evidence to seize and what to examine in detail. Because of the quantities of digital material available—numbers of computers, mobile phones, tablets etc plus the ever-increasing storage capacity each holds, selections have to be made. Police refer to this process as *triage* but insufficient thought has been given to how it executed—and by whom. There seems a very good case for the development of specialist *Digital Scenes of Crime Officers (SOCOs)* as the skills required are outside those routinely available to regular SOCOs or police officers attending a crime.

28. There is also a very good case for *regional hubs of digital forensic expertise* as opposed to each police force having its own unit. This consolidation is already happening. However it is also essential that regular police investigators have easy access to digital forensic technicians so that they can work together when required.

29. A particularly productive route to the investigation of organised groups which deploy cyber techniques appears to be the Covert Internet Investigator (CII). There are a number of courses in CII, for example from Skills for Justice[46] and NPIA[47] but there is as yet no published Code of Practice, which would seem important in developing public confidence in the ethicality and robustness of the methods

30. The use of *private sector out-sourcing of digital forensic services* needs to be deployed with care. There are a number of highly competent companies and individuals, many former police officers and law enforcement agency employees. But there is danger in current practices of aggressive competitive tendering—if a OIC (Officer in Charge) lacks the knowledge fully to formulate his requirement, all that the tendering forensic service provider will do is respond to that tender. If, as now often happens, the OIC and the successful forensic service provider are geographically separated, police and technician will never work properly together and opportunities are missed.

31. Anther often-neglected aspect of law enforcement is the role of the *Crown Prosecution Service*. For some time the CPS has had specialist prosecutors who have enjoyed a certain level of training—indeed I have done a small amount myself. But if my experience is anything to go by most CPS caseworkers lack much knowledge of digital evidence and in particular evidence derived from hard disks. All too often one sees the "particulars" on an indictment that make little or no sense. The fear is that mistakes in the framing charges both generates expense elsewhere in the criminal justice system—showing up in defence criminal legal aid and in court costs—and can sometimes result in the guilty going inadequately punished.

32. As with many issues within law enforcement response to digital evidence the problem is not a total absence of activity but that the extent and quality of resource made available is not keeping pace with the rates at which digital evidence in its various forms of growing throughout society.

33. See also my remarks about evidence from the cloud—paragraph 21 above.

International Dimensions

34. Although getting further international support and sign-up for the CoE Cyber Crime Convention (The Treaty of Budapest, 2001) is an obvious ambition, the Committee needs to be alert to the possibility that in some parts of the world it is perceived as too orientated to the conditions of Western Europe and North America. Alternative initiatives are being developed by the International Telecommunications Union. The Committee, in talking to UK government officials, may want to probe the UK government's stance.

[46] http://nos.ukces.org.uk/NOS%20Directory/NOS%20PDF%20%20Skills%20For%20Justice/ConversionDocuments/SFJCECCO8.pdf

[47] http://www.npia.police.uk/en/578.htm

35. At a practical level much appears to depend on the quality of personal relationships between UK law enforcement specialists and their opposite numbers in other countries. I note the role of SOCA in this regard.

36. A further issue the Committee may like to consider is the position where, although an offence may have been committed within the jurisdiction of the English courts—the Computer Misuse Act, ss 4–5 are quite widely drawn—there are significant difficulties in successful UK prosecution where the vast bulk of the evidence is outside UK jurisdiction. The Crown Prosecution Service currently has a consultation: http://www.cps.gov.uk/consultations/concurrent_jurisdiction_consultation.pdf

Promotion of Public Awareness

37. The investigation of crimes in which digital evidence is an important component will always be expensive. Whatever arguments one has about definitions of e-crime it is unquestionably true that many are transborder in nature. For both of these reasons it is unrealistic to expect successful law enforcement action in anything other than a very small proportion of overall criminal acts. For these reasons prevention and mitigation are critical. It is disappointing that the National Cyber Security Programme placed so little emphasis on helping individuals and businesses help themselves. In the end the best people to apply protection to computers are those who immediately use them. One of the big concerns in E crime is the extent to which social engineering methods are deployed and education is the principal means by which it can spotted and thwarted. I notice that out of a total of £650 million for the overall programme get safe online has received just under £400,000.

38. I hope the committee will consider the virtues of extending the notion of "public health" to the cyber domain. We surely need much more frequent Government-sponsored official advice. Inevitably commercially sponsored advice pushes the public towards the specific products and services of the sponsors.

November 2012

Written evidence submitted by Financial Fraud Action UK [EC 15]

I write in relation to the Home Affairs Committee Inquiry on e-crime and, in particular, the evidence given by Professor Ross Anderson at your hearing on 20 December 2012. We are concerned over the accuracy of several of Professor Anderson's comments and would like the chance to put a more informed view before your Committee's members.

Financial Fraud Action UK is the name under which the financial services industry across the UK co-ordinates its activity on fraud prevention. FFA UK works in partnership with The UK Cards Association which represents credit cards, debit cards and charge cards in the UK. Its members are the leading retail banks and financial institutions in the UK who issue payment cards and extend credit to their customers (the card issuers), and those who process card transactions on behalf of merchants (the merchant acquirers).

During the hearing, Professor Anderson suggested that:

> " ... banks often find it easy to blame their customers for fraud... The banks certainly claim that they will blame people if there was gross negligence. In practice, they often blame people as a routine matter, even when it is not clear there was negligence at all."

The position of the banks is, and always has been, very clear. The innocent victims of fraud can expect to receive full protection against any losses—provided in the form of a full and timely refund, While both banks and cardholders share responsibility for the security of the card, it is only in circumstances where customers have been grossly negligent in protecting their PIN and card that they sustain any loss—which is a high threshold to overcome. Processes embedded by the banks ensure that all customers who are genuine victims of fraud will be refunded and will suffer no loss with the burden of proof on the bank to demonstrate otherwise, The cross-industry picture is that 98% of cases are resolved with a full refund being delivered for the customer. The remaining 2% is made up of a combination of the following scenarios: firstly, fraudulent claims, and secondly where the customer has been found to have acted with such gross negligence as to have practically colluded with the fraudster.

Banks are required to refund the victims of fraud immediately and, as a recent Which? study clearly showed, the vast majority are refunded within a week. On the rare occasions when the situation is not clear cut and the bank needs to investigate further, most card companies ensure that the available balance and interest payments are unaffected whilst the transaction is investigated, which provides support and respite to customers.

The regulatory framework is overseen by the Financial Services Authority, while cardholders have recourse to appeal the decisions of banks to the Financial Ombudsman Service (FOS). All are able to use this additional route to redress where they are unsatisfied with any decision.

While we are confident in the processes in place, we are always open to representations from FOS, where the organisation feels there are systemic industry-wide issues that require extra attention. To this end, we are hoping to meet with the Chief Ombudsman later this year.

Professor Anderson cast doubt, as part of his evidence, on the banks' observance of the Payment Services Regulations 2009, but the figures set out above make clear that the proportion of customers receiving prompt redress is overwhelming. This is backed by research into the customer experience when it comes to fraud refunds: According to an independent study conducted by Accenture in 2012, less than 10% of respondents rated the service from their banks as anything less than *good* or *excellent.*

I would be delighted to give you a more in-depth briefing on FFA UK and the impact we have had. If you would find this helpful, I will ask my office to contact your team and arrange a suitable time.

Katy Worobec
Head of Fraud Control
Financial Fraud Action UK

February 2013

Supplementary written evidence submitted by Financial Fraud Action UK [EC 15a]

I write to thank you for inviting me to appear before the Home Affairs Committee this week, and for the opportunity to discuss the work of Financial Fraud Action UK with your members.

Refunds for Fraud Victims

During the evidence session I promised to provide further information to the Committee on the figures I cited during my submission concerning the number of refunded fraud claims. Financial Fraud Action UK and our partner organisation, The UK Cards Association, conducted a survey of our major UK retail banking members (list below) in advance of this session. The survey ran between 13 March 2013 and 12 April 2013 and collected data on the length of time taken to process fraud refunds during 2012. Our study found that between 96% and 98% of all fraudulent transactions were refunded on either the same day or the following day. On the basis of these findings, no more than 2% of customers receiving refunds have had to wait longer than two days. These figures corroborate that of the Which? survey published in January which found that 98% of fraud claims were refunded, but gives a more up to date picture of the landscape than the Which? survey, which included cases as long as up to five years ago.

Members surveyed:

— Bank of America.
— Danske Bank.
— Bank of Ireland.
— HSBC.
— Bank of Tokyo Mitsubishi.
— Lloyds Banking Group.
— Barclays.
— National Australia Group.
— Capital One.
— Nationwide Building Society.
— CitiBank.
— Royal Bank of Scotland Group.
— Co-operative Banking Group.
— Santander.
— Coventry Building Society.
— Tesco Bank.

E-Crime

I would also like to take this opportunity to reinforce some of the other statistics I shared with you during the session on the changing pattern of e-crime in the UK, from the perspective of e-commerce and online banking.

E-commerce fraud losses (that is, losses on cards used fraudulently over the internet) peaked in 2008 at £181.7 million, a year when total online card spending reached £41 billion. During 2012 e-commerce fraud losses stood at £140.2 million, a year when total online card spending reached £68 billion. Fraud losses for e-commerce have therefore dropped 23% since their peak in 2008, despite a 66% increase in online card spending.

Online banking fraud losses peaked in 2009 at £59.7 million, a year when there were 22.4 million registered users of online banking. During 2012 online banking fraud losses stood at £39.6 million, a year when there were 26.8 million registered users of online banking. Fraud losses for online banking have therefore dropped 34% since their peak in 2009, despite a 20% increase in the number of registered users of online banking.

The National Fraud Authority (NFA) estimates that all types of fraud cost the UK £73 billion in 2011, of which less than 1% consists of banking and card fraud. Total plastic fraud stood at £388 million in 2012, down 36% from its peak at £609.9 million in 2008. Fraud accounts for just 7p in every £100 spent on cards in the UK, against the backdrop of a total of 9.9 billion card transactions in 2012.

Solutions

I feel these figures demonstrate that the broader picture is that we are winning the fight against fraud, notwithstanding a constant need for vigilance in the light of changing modus operandi and developing technologies both on the provider side and in relation to the "attack tools" used by fraudsters.

The banking industry has invested heavily in fraud prevention and detection activity, including £1 billion spent on the roll-out of Chip and PIN and full sponsorship of the Dedicated Cheque and Plastic Crime Unit (DCPCU) which has prevented fraud to the value of £433 million over 10 years. The banking industry has also pioneered new ways of working with the public sector to address fraud, including work with government on public-private fraud intelligence-sharing, and with the National Fraud Authority on consumer campaigns.

The figures around financial fraud, despite progress, remain higher than we would wish and, as the Committee has heard in previous evidence sessions, there is a real concern among our law enforcement partners that stolen funds are being used to bank-roll terrorist groups and support organised criminal gangs involved in the trafficking of people and drugs.

I'd like to reiterate the point I made about the need to streamline ways to share intelligence between law enforcement and the banking industry, and for data to be shared more effectively across borders. If we are to be even more effective in the fight against financial crime then intelligence-sharing across industries and between public and private sector (as well as internationally) is crucial. This should be reflected in the decisions taken around the new data protection regulations stemming from Europe, as well as decisions to be taken on existing Justice and Home Affairs measures.

There is also a need for a greater and more concerted effort from government, the police, and the private sector on consumer education and awareness raising to encourage small changes in consumer behaviour so that we are not "leaving doors and windows open" to online fraudsters, to use the analogy of ACPO's DAC Martin Hewitt. To this end, having successfully run a number of campaigns jointly with the NFA and other sectors, we would ask for the Government to help in bringing other players to the table.

Chip & PIN

Finally, I would like to supplement my response to Dr Huppert's questions on Chip & PIN to state for the record that the use of PIN to authorise a transaction will not in itself preclude a cardholder from receiving a full refund. Victims of card and banking fraud benefit from a legal and regulatory guarantee of being refunded for any losses in a timely manner, irrespective of the nature of the transaction. In general, card payments are a safer way to do business, attracting much greater protections than traditional payments such as cash or cheque.

We are confident in Chip & PIN as a system and believe it is largely responsible for the substantial decline we have seen in card fraud. While we would never be complacent enough to claim that any system is infallible, the evidence our police colleagues are seeing is that cards most commonly become compromised when consumers unwittingly reveal their PIN, for example through common "shoulder surfing" and distraction thefts at ATMs, or by telephone frauds where a criminal posing as a bank staff member or police officer dupe the customer into disclosing his or her details.

I look forward to reading the Committee's e-crime inquiry report, and please do not hesitate to contact me if I can be of any further assistance.

Katy Worobec
Head of Fraud Control
Financial Fraud Action UK

April 2013

Written evidence submitted by Google [EC 17]

I am writing to you to follow up on questions you raised during my evidence session to the Committee as part of your inquiry into E-crime.

YouTube

YouTube provides a forum for people to connect, inform, and inspire others across the globe. Every day, hundreds of thousands of videos are uploaded to YouTube. In fact, 72 hours of video is uploaded to YouTube *every minute.* Because of the massive scale of You Tube, it is simply not possible to pre-screen all of the content.

As I explained during the evidence session, to ensure that our Community Guidelines are followed, we have developed an innovative community policing system that involves our users in helping us to enforce YouTube's standards. Every day, thousands of users report potential violations of our standards by selecting the "Flag" link while watching videos. Once a user flags a video, a manual review is triggered, and content that breaks our guidelines is promptly removed. Our global policy enforcement team reviews flagged content 24 hours a day, seven days a week, routinely removing material that violates our policies.

Once a video that violates our policies is removed from YouTube, it will be blocked from ever being uploaded to YouTube again. Our systems prevent the re-uploading of videos by creating a unique "fingerprint" of every video we remove. If a user tries to upload an identical video again, it is automatically rejected, regardless of whether the user is using a different user or file name. In addition, our policies ensure that users who repeatedly upload material in violation of YouTube's Guidelines have their accounts suspended.

As for the specific content policies that relate to terrorism, our Community Guidelines clearly prohibit videos that promote terrorism, contain hate speech and videos that are posted with the purpose of inciting others to commit violent acts including bomb-making, sniper attacks, or other terrorist acts. We also remove all videos and terminate all accounts known to be registered by a member of a designated Foreign Terrorist Organization (FTO) and used in an official capacity to further the interests of the FTO.

We take this matter very seriously. Hundreds of videos that use the term "Awlaki" and violate our policies have been flagged by the YouTube Community and subsequently removed from the site by our Removals team.

But we are constantly looking to new ways to improve YouTube, most recently by introducing a programme called "YouTube Deputise" where we invite a small set of users who flag policy-violating content regularly and accurately to access more advanced flagging tools. Initial feedback from piloting this programme suggests that it has resulted in a fivefold increase in flagging from these users without diminishing the accuracy.

We have invited the Counter Terrorism Unit, CEOP and SOCA to become part of this new system to assist them in flagging videos to us at scale. We think this will ensure that UK law enforcement bodies are even better equipped to alert us to policy-violating content as and when it is uploaded onto YouTube in the future.

There does remain, however, some videos that cite Awlaki or include his words on YouTube. While we will continue to remove content that incites violence according to our policies, material that is newsworthy or that does not promote violence will remain on the site. Our policies aim to draw a careful line between enabling free expression and religious speech or political speech while prohibiting content that incites violence. We strongly believe that YouTube is a richer and more relevant platform for users precisely because of the diverse range of views it hosts.

Use of Google Ad Grants by UK Charities

Google Ad Grants is a programme whereby any not for profit can apply to receive up to $10k per month of free advertising on our platforms. You can find out more about the programme at www.google.co.uk/grants.

By the end of 2012 we had donated over $33 million to over 11,000 UK charities through giving them this free advertising (including the Samiritans).

Sarah Hunter
Head of UK Public Policy
Google

March 2013

Supplementary written evidence submitted by Google [EC 17a]

Thank you for your letter of 25 March following my evidence session to the Committee in February. The issues raised in the session itself were addressed in my letter of March 19th. To address your additional questions in turn:

Q: *The default setting on Google+ accounts appears to be public. Would there be any merit in changing this so that information is initially only shared with contacts and altered if the user wishes to make their profile public?*

A: On the desktop, the initial default for G+ is to share with no-one. The user has to choose which circles, individuals, or broader choices—public and extended circles—they want to share with. Then their selection is sticky, so that next time they go to share something, those same people, circles, and original choices will appear. So if you wanted to always post to friends, you could just select "friends" the first time you post and then that will remain your default until you change it. For mobile, the firsttime sharing default is with "your circles", so you do need to change this if you want to share otherwise.

Q: *Google's data use and privacy policies state that it collects data about the web pages that service users visit. How long does Google store this information for and how does it make sure it is secure? Does Google share it with third parties? If so how does it vet the security of their systems and personnel?*

A: Like most websites, our servers automatically record the page requests made when users visit our sites. These server logs typically include your web request, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We store this data for a number of reasons, the most important of which are to improve our services and to maintain the security of our systems. We anonymize this log data by removing part of the IP address (after nine months) and cookie information (after 18 months). None of this data is shared with third parties.

Q: *Does Google support Do Not Track technology? Do you think it's important that users should be able to choose privacy above a personally tailored service?*

A: Our top priority is to protect our users' privacy and security, and to give them easy ways to control their information when they use our services. We are constantly innovating to find new ways to assist that effort. We added a Do Not Track option into Chrome, and we'll continue working with industry on a common approach to responding to the Do Not Track feature. Over the past year we have introduced a number of other features that seek to ensure users have more control:

- Introduction of a Cookies Consent Mechanism to users in Europe.
- We published information about how Google uses cookies, the types of cookies used by Google, how we use cookies in advertising and how to manage cookies in your browser.
- We added a feature in Chrome that lets you easily manage cookies—just click on the page/lock icon in the left corner of the omnibox to view and control any website's permissions.
- We implemented the AdChoices icon in the interestbased ads we show in Europe.

Q: *How many successful hacks have been made against Google in the last year and what types of data were stolen?*

A: None that we know of, and we look really hard. Our security teams and systems are highly effective at fending off attacks—we have actually detected real attempts that failed. Our security team runs frequent tests to estimate how well we're doing at this detection. We also care about and seek to prevent attacks against our users, through phishing or other means, even when the attack is not directed at Google.

Sarah Hunter
Head of UK Public Policy
Google

April 2013

Written evidence submitted by the British Bankers' Association [EC 20]

Thank you for your invitation to provide evidence to the Home Affairs Committee on 16 April. I welcome the opportunity to brief the Committee on the work of the BBA and our member banks to address cyber enabled financial crimes. To inform the discussions, I thought it may be helpful to provide some advance information to the Committee on:

- Supporting bank customers and victims of cyber enabled frauds.
- The evolving nature of cyber threats.
- The challenges in responding.
- The strategic industry approach to financial crime.
- Issues for future consideration.

Supporting Bank Customers and Victims of Cyber Enabled Frauds

BBA members have put in place highly sophisticated security and prevention measures to safeguard customers from online frauds. Banks have also invested in intelligence and analysis systems, recruitment of skilled staff and firm wide training and policies to ensure the most effective strategic defences against financial crimes, as well as working closely with UK law enforcement. These efforts have been essential for driving down online banking fraud losses but also important for maintaining confidence in online banking, particularly given that many customers now use this channel.

Our members see supporting the innocent victims of fraud as a crucial priority. The vast majority of customers that have been defrauded are refunded in accordance with regulatory requirements and banks also provide practical advice and support as appropriate. At the industry level, the BBA works closely with our members to promote best practice for addressing financial crimes including through the guidance materials that we publish.

BBA members are highly committed to raising customer awareness of fraud risks and the "self protection" measures that can be taken. Many banks provide fraud prevention advice on their websites and a number of firms hold awareness raising events for customers. At the industry level, Financial Fraud Action UK (FFA UK) lead fraud prevention efforts on behalf of retail banks and card issuers and have managed a number of awareness raising campaigns including:

- A national campaign, led by FFA UK and supported by the BBA, to raise awareness of the risks posed by criminals that coerce or dupe members of the public into acting as "money mules".
- A partnership[48] between the National Fraud Authority (NFA) and FFA UK that highlighted how cyber criminals steal and use personal information for the purposes of fraud.
- Advice sheets produced jointly by the BBA, FFA UK and the Police, to raise customer awareness of the risks posed by Investment Fraud and a leaflet setting out advice for visitors to Britain.

The Evolving Nature of Cyber Threats

BBA members have achieved good success in driving down the losses from online banking fraud. However, given the size of the British banking sector and the ever growing number of people who conduct their banking and everyday business online, we recognise that our customers will continue to be targeted by cyber criminals. For example, criminals use stolen genuine card details to make fraudulent purchases over the internet via a PC, smart phone or tablet. Criminals also use malicious software and/or "phishing" emails as a means to compromise or steal customers' sensitive banking credentials to enable fraud and money laundering. Criminals also communicate with each other online to trade data and to share knowledge on offending methods.

As banks have strengthened their controls against cyber enabled financial crimes, the criminals have sought to develop new cyber techniques, such as online social engineering, to dupe or coerce people into divulging personal information or making payments. There is also evidence that criminals are targeting other sectors and businesses that may have weaker controls than banks, to access customer information that can be then used for fraud offending.

Cyber techniques may also be used for attacks against banks that are not financially motivated including:

- *Subversion* (often known as "hactivism", this is generally carried out as part of a protest. The attackers seek to expose perceived injustice, bad practise and/or exploitation by banks in order to damage their reputation or force changes in policies).
- *Sabotage* (to disrupt the availability of banks online services and content thus eroding customer trust and damaging the organisations reputation).
- *Espionage* (to steal and exploit sensitive information or intellectual property).

Challenges in Responding to these Threats

Whilst BBA members have developed some of the strongest financial crime controls anywhere in the world, there are significant challenges that remain in responding to the cyber criminals including:

- *Rapid evolution in criminal techniques*—Criminals are adopting new cyber offending techniques in response to the counter measures that are put in place, quickly spotting new opportunities and often operating through organised global networks. Highly advanced analytical capabilities are needed in banks, alongside effective intelligence arrangements with law enforcement, to keep up-to-speed with this rapidly changing threat picture.
- *Balancing customer service and financial crime prevention*—There is a challenge in balancing effective measures for spotting and stopping financial crimes with good customer service, as some necessary control measures can cause delays. Our members are constantly striving to ensure that they have the most effective policies and practice in this respect, as well as providing as much information as possible to customers.
- *Conflicting policies and laws*—Compliance with financial crime obligations can at times conflict with other legal obligations on banks. For example, data protection requirements pose challenges to the efficient sharing of information by banks that is needed to spot and stop financial crimes. Similarly, banks are required by the Proceeds of Crime Act to ensure that they do not "tip off" customers that an investigation is taking place whilst also meeting customer demands for detailed explanations when actions have been taken on accounts.
- *Enforcement capabilities*—Often the investigation and prosecution of criminal cases involving cyber crime can be complex, lengthy and expensive, especially where offenders are located outside the UK. Adequate resources are therefore needed to ensure law enforcement is able to provide an effective response to cyber crime cases reported by banks and their customers. This is vital not only for ensuring that justice is served to victims but also to deter potential future offenders.

[48] "The Devils in your Details" campaign

The Strategic Industry Approach to Addressing Cyber Enabled Financial Crimes

The role of the BBA

The BBA, as the leading association for the banking and financial services sector, supports our members' efforts to address all forms of financial crime[49] by coordinating strategy and policy, providing guidance, promoting best practice and facilitating operational interaction between banks and law enforcement. The following are some examples of our work in 2012 on fraud matters:

— *Thought Leadership:* We provided a report to the NFA in April 2012 setting out an industry perspective on international fraud threats and challenges, including recommendations for enhanced cooperation between banks and HM Government in this area. The Chief Executive of the NFA in his written response described our report as *"well written" and "an example of where work conducted by one sector can highlight wider issues and identify joint working opportunities between other sectors and organisations…..".*

— *UK Policy:* In August 2012 the BBA responded to the FSA Guidance Consultation on "Banks defences against investment fraud". Since our response we have agreed a programme of work with our members to follow up on the FSA recommendations and we are also liaising with the Financial Conduct Authority on this matter. Through 2012 we also provided views to the Home Office on the fraud intelligence arrangements for the National Crime Agency and to the Department of Work and Pensions on the financial crime controls for the Universal Credit.

— *International Policy:* As well as responding to a number of EU level consultations, the BBA supported United Nations work on financial crime in 2012. This included participation in the UN Experts Group on Economic Crime and Identity Fraud and support for an initiative to promote financial crime compliance in the EurAsia region.

— *Industry Analysis:* In December 2012 we provided a report[50] to BBA members setting out analysis of cyber threats and challenges as a basis for strengthened industry collaboration in this area (more details on work in this area are set out below).

— *Operational/practical support:* In early 2012 the BBA established a mechanism with the Metropolitan Police to ensure the most efficient exchange of information with BBA members to prevent financial crimes during the Olympics. Later in 2012 we agreed a new arrangement for the National Fraud Intelligence Bureau to provide fraud alerts to investment banks and smaller banks through an online system managed by the BBA.

The BBA Financial Crime Strategy 2013–14

Our members recognise the importance of collaboration across the industry on financial crime. With this in mind, the BBA Board in October 2012 agreed a two year strategy to address financial crime comprising the following priority initiatives:

— *An Annual BBA Financial Crime Report* to publicly outline how the industry is responding to financial crime, the challenges we face and our future priorities.

— *A review of industry intelligence arrangements* for financial crime, to enhance industry knowledge of emerging financial crime risks.

— *Dialogue with the Home Office* on BBA proposals for improvements to the legal and policy framework for financial crime and on bank partnership with the National Crime Agency.

— *Proactive engagement with the Financial Conduct Authority* to support our members to understand and meet Regulatory expectations on financial crime.

— *Intensified BBA led engagement with EU and international bodies*, to promote public/private partnerships at the global level to address financial crimes.

The BBA Financial Crime Policy Group acts as our key oversight committee for delivery of the strategy, though regular reports will be provided to the BBA Board over the coming years. Consideration of cyber crime is an intrinsic element of our strategic approach in this area given that criminals employ cyber techniques for a range of financial crimes, particularly fraud and money laundering. The BBA has also recently established a new dedicated Cyber Advisory Panel, bringing together senior bank representatives to coordinate industry strategy and policy on strategic cyber security and cyber risk management issues.

Our partnership with Financial Fraud Action UK

The BBA works closely with FFA UK to support our members' efforts to address cyber enabled frauds. Key areas of collaboration include:

— *Campaigns to raise customer awareness of fraud* and promote bank best practice.

— *Promoting the sharing of knowledge and expertise* within the banking sector on emerging fraud threats.

[49] Our portfolio includes work to tackle bribery, corruption, fraud, money laundering, terrorist financing, cyber crimes and physical crimes.

[50] BBA report titled "*Defining the cyber threats and challenges to the banking sector*"

— *Developing common approaches on fraud policy issues*, including joint representations to UK and international bodies where appropriate.

The FFA UK and the BBA will continue to work together to promote effective fraud prevention and raise customer awareness of emerging risks. Whilst the BBA and FFA UK have some common retail bank members the BBA also is keen to further ensure that investment bank, smaller bank and private bank members are brought into industry level initiatives where appropriate.

Areas for Future Consideration

The BBA welcomes the proactive approach of HM Government to engagement with the private sector on cyber crime matters. In particular, the BBA is pleased to be participating in the recently formed Cyber Crime Reduction Partnership that brings together industries, HM Government and academia to develop collaborative efforts to address cyber crimes.

Beyond this, we would suggest that the following could be considered to strengthen our collective capabilities to address cyber offending:

Intensified public awareness campaigns

Whilst recent banking industry led campaigns have successfully raised public awareness of cyber crime risks, there is a need for an intensified multi-sector approach to ensure that members of the public better understand the threats they face. Further targeted campaigns are needed to ensure that prevention messages are reaching key audiences, such as younger online users and the vulnerable.

Reforms to the legal and policy framework

BBA members are of the view that government should consider possible improvements to the legal and policy framework for financial crime. Specifically there may be merit in considering updates to the Proceeds of Crime Act, to ensure it is up-to-date with modern financial crime offending techniques. Policy or legislative change may also support a more effective balance between data protection obligations and the requirement for firms to share information to address financial crimes.

Enhanced investigation and enforcement capabilities

The establishment of the National Crime Agency is a real opportunity to develop the highest quality capabilities for investigation and enforcement against cyber offenders. BBA members are keen to support the strengthening of enforcement capabilities by putting in place the strongest possible information exchange mechanisms and through the exploration of potential “two-way” sharing of staff between the National Cyber Crime Unit in the NCA and BBA member banks.

A coordinated global partnership

Given the global nature of cyber offending and the widespread harm it causes, the BBA is of the view that a coordinated international multi-sector approach is required. The UN Experts Group on Cyber Crime may provide a useful mechanism for international policy development but we believe that beyond this can be done globally at a practical level. This could include sharing of knowledge between different sectors to enhance understanding of emerging cyber offending techniques, improvements to international standards for addressing cyber crimes and the promotion of greater public awareness of cyber crime risks.

I hope this provides useful supporting information to the Committee and I look forward to discussing these issues further on 16 April.

Anthony Browne
Chief Executive
British Bankers’ Association

April 2013

Written evidence submitted by Facebook [EC 21]

Further to your letter of 25 March 2013, I have provided further information from Facebook relating to your inquiry:

1. *Facebook user numbers in the EU:* Facebook does not provide public data on the number of active Facebook users in the European Union as a whole. However here are the monthly active user numbers for the largest five markets in the EU made public at the time of our most recent quarterly results:

UK 33 million.

France 26 million.

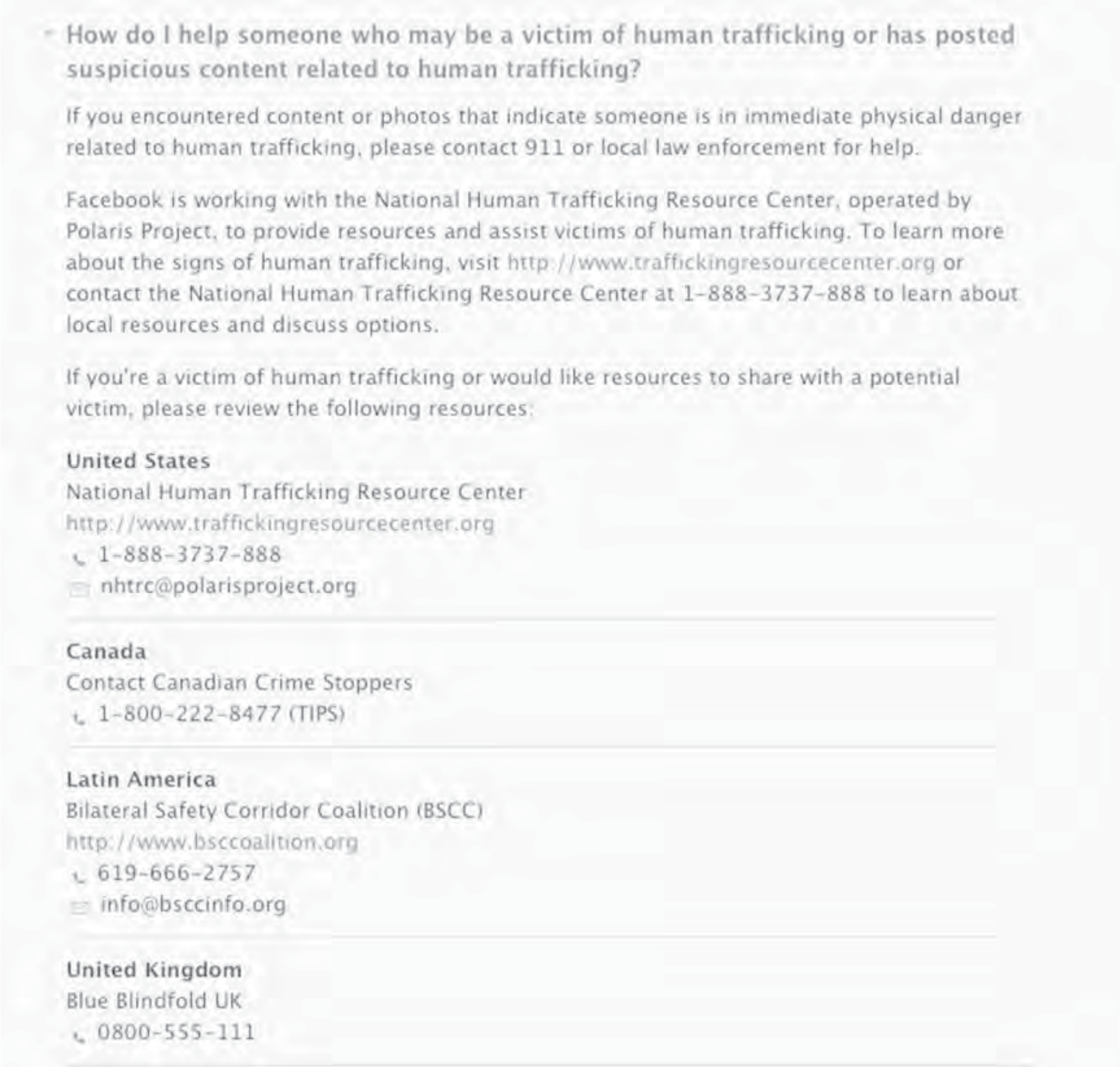
Germany 25 million.

Italy 23 million.

Spain 18 million.

2. *HTC phone and pre-installed Facebook features:* In retrospect, Mr Ruane's question was probably prompted by press speculation about a product launch, which was pure speculation on the day of the hearing itself. On 4 April 2013, Facebook announced the launch of Facebook Home. This will come preinstalled on HTC phones in the US. It can be turned off at any point by the user and can also be uninstalled at any time. When Facebook Home is active, we will log information about the user's activity on Facebook's suite of products. In addition to the standard information we log with all our apps, we will also log notifications and app information when they interact with Facebook Home. We do not log or track the user when they use apps independent of Facebook on the phone.

3. *People reporting crime on Facebook:* While Facebook makes it easy for people who use our service to report potential abuse or violations of our terms of service, we do not have any specific data which relates to the Committee's question about reports of crime. Instead our Help Centre advises users to contact local law enforcement if they wish to report a crime. An example of that advice is shown in the screenshot below, from the Help Centre, relating to human traffic:



How do I help someone who may be a victim of human trafficking or has posted suspicious content related to human trafficking?

If you encountered content or photos that indicate someone is in immediate physical danger related to human trafficking, please contact 911 or local law enforcement for help.

Facebook is working with the National Human Trafficking Resource Center, operated by Polaris Project, to provide resources and assist victims of human trafficking. To learn more about the signs of human trafficking, visit http://www.traffickingresourcecenter.org or contact the National Human Trafficking Resource Center at 1-888-3737-888 to learn about local resources and discuss options.

If you're a victim of human trafficking or would like resources to share with a potential victim, please review the following resources:

United States
National Human Trafficking Resource Center
http://www.traffickingresourcecenter.org
☎ 1-888-3737-888
✉ nhtrc@polarisproject.org

Canada
Contact Canadian Crime Stoppers
☎ 1-800-222-8477 (TIPS)

Latin America
Bilateral Safety Corridor Coalition (BSCC)
http://www.bsccoalition.org
☎ 619-666-2757
✉ info@bsccinfo.org

United Kingdom
Blue Blindfold UK
☎ 0800-555-111

4. *Data collected when people use other sites:* All the questions raised under this point are addressed in considerable detail in two reports of the Office of the Irish Data Protection Commissioner (I-DPC) in December 2011 and September 2012, which can be accessed at the links below, including detailed, independent technical appendices. Both reports and their technical appendices were published in full.

http://www.dataprotection.ie/docs/Facebook_Ireland_Audit_Report_December_2011/1187.htm

http://www.dataprotection.ie/docs/Appendices_to_Facebook_Ireland_Audit_Report_Dec_2011/1188.htm

http://www.dataprotection.ie/docs/21–09–12—Facebook-Ireland-Audit-Review-Report/1232.htm

In summary:

- Facebook's Data Use Policy states that we delete or anonymize data collected through social plugins on other sites within 90 days. This has been verified by the I-DPC.
- The I-DPC reviewed Facebook's data security operations and concluded that: *It is important to state at the outset that as could be expected FB-I places an enormous and ongoing focus on the protection and security of user data. Our audit has confirmed this focus. (December 2011 report, para 3.9.4)*
- And further: *The majority of the controls described by FB-I appeared to this Office to be effective. It can be reasonably concluded that if large-scale, frequent data breaches were taking place on Facebook's corporate networks, that this would be widely reported, particularly considering Facebook's global profile. Since this is not the case, the information security controls in Facebook appear to be preventing these types of incidents. (ibid, para 3.9.6)*
- Facebook does not share information collected via social plugins with third parties over and above the information shared by an individual making use of those websites. This extract from our Help Centre makes this clear and explains the reasons we collect this information:

What information does Facebook get when I visit a site with the Like button or another social plugin?

If you're logged in to Facebook and visit a website with the Like button or another social plugin, your browser sends us information about your visit. It's important to note that Facebook is not retrieving this information. Rather, since the Like button is a little piece of Facebook embedded on another website, the browser is sending information about the request to load Facebook content on that page.

We record some of this information for a limited amount of time to help show you a personalized experience on that site and to improve our products. For example, when you go to a website with a Like button, we need to know who you are in order to show you what your Facebook friends have liked on that site. The data we receive includes your user ID, the website you're visiting, the date and time and other browser-related information.

If you're logged out or don't have a Facebook account and visit a website with the Like button or another social plugin, your browser sends us a more limited set of information. For example, because you're not logged into Facebook, you'll have fewer cookies than someone who is logged in. Like other sites on the internet, we receive information about the web page you're visiting, the date and time and other browser-related information. We record this information for a limited amount of time to help us improve our products. For example, we sometimes find bugs in the systems we've built to gather aggregate data on how people are interacting with sites that use the Like button or other social plugins. It's helpful to be able to reference this anonymized information when investigating these bugs so we can find their sources and fix them quickly.

As our Data Use Policy indicates, we use cookies to show you ads on and off Facebook. Regardless of whether or not you're logged in, we don't use the information we receive when you visit a site with the Like button or another social plugin to create a profile of your browsing behavior on third-party sites to show you ads. However, we may use anonymous or aggregate data to improve ads generally and information we receive to study, develop or test new and existing products or services. We delete or anonymize the information we receive within 90 days, and we don't sell it to advertisers or share it without your permission.

5. *Do Not Track (DNT):* Facebook believes in the importance of user control of data about them and therefore we are supportive of the efforts of stakeholders, including at the World Wide Web Consortium and the Digital Advertising Alliance, to develop a standard for DNT that will enable people to control their information as they browse the web. We are actively involved in those industry-wide discussions, which cover many difficult technical questions that will need to be resolved before any DNT standard can be adopted.

6. *Review processes for Facebook apps:* Facebook provides extensive information to users in respect of applications, including the data being shared with each application upon its installation. Applications can only be installed once the user has given permission for such sharing. The policies which developers have to comply with are clear and we take a number of steps to enforce them. Our actions in this respect were audited by the I-DPC and this excerpt from the audit report summarises the I-DPC's assessment:

> *"The role of Platform Operations is to enforce Facebook's Platform Policy, interacting with developers of third party apps and developers using the social graph, ie, social plugins, to ensure adherence to Platform Policy. An examination was conducted of the work queues of the Platform Operations Team. It was noted that Facebook has now introduced a number of automated tools, developed in Dublin, to proactively and automatically identify and disable applications engaged in inappropriate activity such as spamming friends or friends of friends, excessive wall posting, etc. The Team also responds to specific user complaints regarding the behaviour of applications and enforces a graduated response against the application and the application provider depending on the nature of the contravention of the Platform policy. We examined one complaint from a user in relation to unauthorised use of Intellectual Property by another developer which was received on 9 November and action was taken to delete the application within 2 hours. The account of the developer was disabled and all other applications which they had developed were also subjected to*

> *review. We also examined a phishing complaint received from a user who reported an application trying to retrieve their email and password. The application was immediately disabled and further action taken. It was also pointed out that in line with Facebook's real name culture that all applications (even those developed by the large games developers) must be developed by and attributable to an identifiable user on Facebook." (December 2011 report, para 3.6.5)*

7. *Reports of hijacked accounts or scams:* Anyone believing that their account has been hijacked or hacked is advised on our Help Centre to go to: www.facebook.com/hacked where they can manually lock down their account with immediate effect, reset their password and take other steps to secure their account. Any user reporting that their friend's account may have been hacked is provided with the same advice—ie their friend should take these steps. We also take a number of preventative steps to guard against the possibility of an account being hacked:

- *Recognised devices:* Facebook allows people to register devices that they use Facebook on regularly.
- *Remote log-out:* If someone forgets to log out of Facebook, they can remotely log off any live session they have running by accessing this tool in their security settings.
- *Secure browsing:* Facebook encourages all users to turn on secure browsing for added protection (add "s" to the end of http in their browser address).
- *Login notifications:* We send notifications every time an account is accessed from an unsaved device.
- *Login approvals:* If someone logs in from an unsaved device, we will send a code to their registered mobile phone to authorize that log-in.

8. *Hacks against Facebook:* Security is a top priority for us, and we devote significant resources to protecting people's accounts and information. We maintain a strong relationship with security experts around the world and work closely with them in the rare instances in which they find vulnerabilities on Facebook. We've created a simple form for these people to contact us that we link to both from our Help Centre and from the "Whitehats" tab on the Facebook Security Page https://www.facebook.com/whitehat. We also recently rewrote our responsible disclosure policy to make it even easier for researchers to let us know when they find a vulnerability, so we can fix it quickly and before it is exploited.

I hope that this further information is useful to the Committee.

Simon Milner
Policy Director, UK
Facebook

April 2013

Printed in the United Kingdom by The Stationery Office Limited
07/2013 029956 19585