House of Commons

Science and Technology Committee

Malware and cyber crime

Twelfth Report of Session 2010–12

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/science

Ordered by the House of Commons to be printed 25 January 2012

HC 1537
Published on 2 February 2012
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

Science and Technology Committee

The Science and Technology Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Government Office for Science and associated public bodies.

Current membership

Andrew Miller (*Labour, Ellesmere Port and Neston*) *(Chair)*
Gavin Barwell (*Conservative, Croydon Central*)
Gregg McClymont (*Labour, Cumbernauld, Kilsyth and Kirkintilloch East*)
Stephen McPartland (*Conservative, Stevenage*)
Stephen Metcalfe (*Conservative, South Basildon and East Thurrock*)
David Morris (*Conservative, Morecambe and Lunesdale*)
Stephen Mosley (*Conservative, City of Chester*)
Pamela Nash (*Labour, Airdrie and Shotts*)
Jonathan Reynolds (*Labour/Co-operative, Stalybridge and Hyde*)
Graham Stringer (*Labour, Blackley and Broughton*)
Roger Williams (*Liberal Democrat, Brecon and Radnorshire*)

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

Publications

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 http://www.parliament.uk/science. A list of reports from the Committee in this Parliament is included at the back of this volume.

The Reports of the Committee, the formal minutes relating to that report, oral evidence taken and some or all written evidence are available in printed volume(s).

Additional written evidence may be published on the internet only.

Committee staff

The current staff of the Committee are: Mrs Elizabeth Flood (Clerk); Dr Stephen McGinness (Second Clerk); Dr Farrah Bhatti (Committee Specialist); Xameerah Malik (Committee Specialist); Andy Boyd (Senior Committee Assistant); Julie Storey (Committee Assistant); Henry Ayi-Hyde (Committee Office Assistant); and Nick Davies (Media Officer).

Contacts

All correspondence should be addressed to the Clerk of the Science and Technology Committee, Committee Office, 7 Millbank, London SW1P 3JA. The telephone number for general inquiries is: 020 7219 2793; the Committee's e-mail address is: scitechcom@parliament.uk.

Contents

Report

Summary

The internet can be a confusing place and that provides opportunity for criminals and criminal behaviour. High profile cases of criminal behaviour tend to be those that involve large sums of money or threaten national security. There are however dangers for everyday users of the internet that are often lower down the priority agenda for regulators, legislators and the police.

The Government has been working to address the issue of cyber crime and published its *Cyber Security Strategy* at the end of last year, while we were taking evidence on this inquiry. We welcome the broad sweep of the strategy but it remains, in essence, focussed at too high a level to address the key concerns of everyday internet users.

The overwhelming message from those who gave evidence to us was that there is a need for computer users to be better informed. Those using the internet need to be aware of the potential risk and have a trusted source of authoritative advice and up to date information about malware and internet scams. Too often advice and information for the internet are too technical or difficult for most computer users to properly understand and effectively act upon. There is also the problem that there are so many messages from a variety of sources that it is easy to become overwhelmed and difficult to know who to trust.

The Government already sponsors the Get Safe Online website but we believe this site is in need of substantial investment and improvement. Get Safe Online needs a much higher profile among UK computer users and the Government is central in that awareness raising, through integrating the site with relevant official organisations and governmental bodies and providing a one-stop shop for victims of cyber crime to report that crime and get authoritative information on how to remedy their situation.

One key element that the Government can address is that of providing a way for consumers to recognise those computer programmes that enhance rather than undermine online security. We have recommended that the Government seek to develop a kite mark, or similar solution, that software publishers can be awarded if they prove their product meets security standards. However, we recognise such schemes can militate against smaller companies and ask the Government to investigate how it might remove some of the financial disincentives for smaller companies wanting to promote the security of their products.

We believe that the Government has a duty to protect the people of the United Kingdom from crime regardless of whether that crime takes place on the streets or on the internet. We consider that victims of crime should expect to be able to take those crimes to their local police and to be given good advice on useful steps to recover from the impact of that crime. Towards that end we recommend that the Government take steps to improve general knowledge about cybercrime among all policemen in the UK as well as focussing on the specialist units as outlined in the *Cyber Security Strategy*.

1 Introduction

The need to address malware and cyber crime

1. The Government has defined malware as software written with malicious intent.[1] Thus the elements of a piece of malware may legitimately be used as software as long as there is no malicious intent.

2. The BCS,[2] in their submission, outlined the variety of ways in which malware could have an impact on individual computer users.

- The PC[3] becomes part of a Botnet[4] (maybe thousands or tens of thousands of individual computers), which is then used by criminals to distribute Spam email to others, or to launch a denial of service attack against an organisation. Botnets are increasingly rented out for criminal purposes. The owner of the PC may only suffer a loss in performance of their PC or they may be accused of committing a criminal offence.

- The malware may be used to extract useful information that may be stored on the PC, which could include personal details, bank details etc. For example, the Government said in December 2010 that it had been a victim of the Zeus malware, with undisclosed loss of sensitive information. The loss of information can have serious consequences for the individual concerned, not only financial loss, but also by affecting their relationships with others or cause the loss of irreplaceable records such as personal photographs.

- The PC may be used to host illegal content, such as child pornography. The owner of the PC is then open to the accusation of knowingly hosting the illegal content.[5]

3. BCS indicated that there were no authoritative statistics on how many PCs are infected in the UK: estimates vary between one and fifteen percent. In their opinion, 5% would be a conservative estimate.[6] Symantec told us that 38% of respondents to the latest Norton Cyber crime Report[7] had suffered a malware related incident, over half of those within the 12 months preceding the survey. Malware was the most common form of cyber crime experienced, followed by online credit card fraud and social network profile hacking.[8]

4. The McAfee Threat Report for the third quarter of 2011 showed that mobile phone malware had doubled since 2009 and that the majority of new malware on mobile platforms had been targeted at android phones. Malware for mobile phones, with total

[1] Ev 23, para 3

[2] Formerly the British Computer Society, now BCS, the Chartered Institute for IT

[3] PC—usually used to denote a personal computer running a Microsoft operating system

[4] Botnet—a network of compromised PCs that may be used by the malware author for criminal purposes

[5] Ev 36, para 4

[6] Ev 36, para 4

[7] Norton Cyber crime Report 2011 http://uk.norton.com/content/en/uk/home_homeoffice/html/cybercrimereport/

[8] Ev w24, para 20

detected variants numbering just over 1200, remained a small element in overall malware statistics as over 4 million new malware variants for PCs were detected by McAfee in the third quarter of 2011 alone.[9]

5. Newspapers find any cyber crime a fascinating topic, despite the fact that the crimes perpetrated are usually traditional ones such as fraud or theft, with the internet or email being merely the instrument of the crime.[10] The main focus of media interest, however, is on the large scale attacks on companies or government agencies which would constitute threats to national security. A recent example was a report that a US water utility had been a victim of hacking and the hackers had been able to damage the pumps in that utility.[11] These stories portray a scenario of shadowy enemies striking from hidden locations to threaten civilisation, reminiscent of cold war propaganda. They are not always well-founded—for example the FBI have indicated that they could not confirm intrusion in the water company system and that they 'concluded that there was no malicious or unauthorised traffic from Russia or any foreign entities, as previously reported'.[12]

6. Recent news stories cover a wide range of other cyber crime incidents. In August there were reports of companies being defrauded as international phone calls were re-routed through their company switchboards.[13] In September a Dutch firm, DigiNotar, was widely reported as filing for bankruptcy after being hacked.[14] In October the *Guardian* reported on a new Stuxnet[15] worm targeting companies in Europe.[16]

7. However, the majority of 'e-crime' is less dramatic but more pervasive. Dr Richard Clayton told us that

> … in the most general terms [...] the eco-system for mass-market criminality is based on spam sent by botnets, and those botnets are constructed by compromising end-user machines with malware.[17]

8. BCS referred us to a survey by the Ponemon Institute showing that the cost of data breaches of UK organisations had increased for a third year running. They reported the average data breach to cost £71 per record accessed, with the highest overall cost reported being £6.2 million.[18] These costs included detection and escalation of the data breach, notification of those affected, the cost of responding to the breach and the cost of lost business.

[9] McAfee Labs, *McAfee Threats Report: Third Quarter 2011*, 2011 www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf

[10] For example, "Fraudsters are costing shoppers £7bn, say MPs", *The Daily Telegraph*, 9 November 2011

[11] "Hackers 'hit' US water treatment systems", *BBC online*, 21 November 2011, www.bbc.co.uk/news/technology-15817335

[12] "FBI plays down claim that hackers damaged US water pump" *BBC online*, 23 November 2011, www.bbc.co.uk/news/technology-15854327

[13] "Businesses hit by new cybercrime", *BBC Online*, 15 August 2011, www.bbc.co.uk/news/uk-england-14533738

[14] For example, "DigiNotar files for bankruptcy in wake of devastating hack", *Wired*, www.wired.com/threatlevel/2011/09/diginotar-bankruptcy/

[15] Stuxnet is a computer worm, discovered in June 2010, that initially spreads via Microsoft Windows and targets Siemens industrial software and equipment.

[16] "New Stuxnet worm targets companies in Europe", *Guardian*, 19 October 2011

[17] Ev 31, para 18

[18] Ev 36, para 4

9. The Norton *Cybercrime Report* showed that while three times more adults surveyed suffered cyber crime than offline crime over the past 12 months (44% online compared with 15% offline) only three in ten of them thought they were more at risk online than offline. Norton reported 1 million cyber crime victims a day over the 24 countries surveyed.[19] The Commtouch *Internet Trends Threat Report 2011* also pointed out that malware attached to emails was a rising trend. Commtouch provides security vendors with proactive email-borne virus detection that analyses over 2 billion emails per day: it found that in March 2011 over 30% of emails analysed had attached malware.[20]

10. The Government, in response, published its *Cyber Security Strategy* on 25 November 2011.[21] Francis Maude, the Minister for the Cabinet Office and Paymaster General, indicated how he expected the strategy to tackle cyber crime and promote a more informed citizenry:

> This strategy also outlines our plans for a new cybercrime unit with the National Crime Agency, to be up and running by 2013. This unit will build on the groundbreaking work of the Metropolitan police's e-crime unit by expanding the deployment of "cyber-specials", giving police forces across the country the necessary skills and experience to handle cybercrimes. We will also ensure that the police use existing powers to ensure that cybercriminals are appropriately sanctioned as well as introducing a new single reporting system to report financially motivated cybercrime through the existing Action Fraud reporting centre.
>
> [...]
>
> Prevention and education are also crucial. Get Safe Online is a very good example of how Government, industry and law enforcement can work together to address this issue and improve the website by early 2012. In addition, we will work with ISPs to seek a new voluntary code of conduct to help people identify if their computers have been compromised and what they can do about it.[22]

Previous work

11. On 2 March 2011, we published the report, *Scientific advice and evidence in emergencies*, to examine how scientific advice and evidence is used in national emergencies, when the Government and scientific advisory system are put under great pressure to deal with atypical situations.[23] The threat of an online attack where national security might be threatened was one scenario which we considered. This inquiry focussed, however, on national security rather on the impact on individual citizens or on the structure of policing of cyber crime.

[19] Symantec, *Norton Cyber crime Report 2011*, September 2011 uk.norton.com/content/en/uk/home_homeoffice/html/cybercrimereport/

[20] Commtouch, *Internet Threats Trend Report*, April 2011

[21] Cabinet Office, *Cyber Security Strategy*, 25 November 2011

[22] HC Deb, 25 November 2011, c38–9WS

[23] Science and Technology Committee, Third Report of Session 2010–12, *Scientific advice and evidence in emergencies*, HC 498

12. The Government has also been active in looking at national security and the threat of cyberattack on the UK. The Government organised a conference bringing organisations from all over the world to discuss the issues and how to improve resilience to cyberattacks.[24] The Government's *Cyber Security Strategy* (mentioned in paragraph 10 above) also addresses these high level problems but also sets out how individual computer users and small businesses might be protected from the impact of crime committed through malware.

Our inquiry

13. We announced our inquiry on 19 July 2011 and issued a call for evidence based on the following terms of reference:

- What proportion of cyber-crime is associated with malware?
- Where does the malware come from? Who is creating it and why?
- What level of resources are associated with combating malware?
- What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?
- Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?
- How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

14. We received 22 submissions in response to our call. We would like to thank all those who submitted written memoranda.

15. In November 2011 we held two evidence sessions during which we took oral evidence from three panels of witnesses, to whom we are grateful:

> On 9 November 2011 we took evidence from: Dr Richard Clayton, Research Assistant, University of Cambridge, Professor Peter Sommer, Visiting Professor in the Department of Management, London School of Economics, and Dr Michael Westmacott, BCS, the Chartered Institute for IT but also representing Royal Academy of Engineering & Institution of Engineering and Technology.
>
> On 14 November 2011 we took evidence from two panels. First: Gordon Morrison, Director of Defence and Security, Intellect, Janet Williams, Deputy Assistant Commissioner, Charlie McMurdie, Detective Superintendent, Head of Police Central e-Crime Unit, Metropolitan Police, and Lesley Cowley, Chief Executive, Nominet; followed by James Brokenshire MP, Parliamentary Under-Secretary of State for Crime and Security, Home Office.

[24] London Conference on Cyberspace, QEII Centre, 1-2 November 2011

We would also like to thank Symantec and McAfee for providing an informal opportunity for us to get practical experience of malware and a clearer perspective on the extent of the associated problems.

16. We begin our report with an overview of the impact of cyber crime on individuals and small businesses along with an examination of the role of the police in tackling cyber crime. We go on to examine the defences available to individuals and what should be done to ensure that the average UK citizen becomes more aware of cyber crime and is able to take necessary self-protection measures.

2 Cyber crime and Policing

Individual Exposure and Knowledge

17. When a computer is enabled to access the internet, that machine becomes part of the network; but access to the internet is not necessarily one-way: anyone with the right skills may be able to access the machine and its contents, to monitor anyone who uses that machine and possibly to co-opt the machine into a network of similarly compromised machines that facilitates further criminal activity. The Serious Organised Crime Agency told us that a:

> significant proportion of cyber-crime uses malware to perform some part of the crime. Even spamming now involves the use of malware, as the majority of spam messages are now delivered using Botnets.[25]

18. Exposure to the possibility of crime is not uncommon. What makes cyber crime different is that many people have not developed an understanding of what constitutes risky behaviour, how to minimise that risk and what to do if they become a victim.

19. Crimes committed on the internet are often the bread and butter crimes of everyday criminal activity: fraud and theft. The driver for criminal activity on the internet, like everyday street crime, is gaining money. The *Cost of Cyber crime* report by the Cabinet Office outlines the costs to individual computer users: "£1.7bn for identity theft, £1.4bn for online scams and £30m for 'scareware'."[26]

20. There is a suggestion in Home Office statistics that use of the internet increases exposure to credit card fraud:

> A supplementary document to the British Crime Survey was published by the Home Office in May 2010. It looked at data from 2008–09 and found that 6.4% of credit card owners were aware of fraudulent use of their card over the previous 12 months. Victimisation rates were higher at 11.7% for incomes over £50,000/annum. If the Internet had been used at all (irrespective of income) the rate was 7.7% and if the Internet was used "every day" then it was 8.9%. In contrast, the 2010/11 British Crime Survey found that burglary affected just 2.6% of households and thefts from cars affected 4.2% of households.[27]

21. We have been told several times, however, that the data on cyber crime is not reliable or authoritative as it is not systematically recorded. Dr Richard Clayton said that "until we have reliable data we will not be able to assess the size of the cyber crime problem nor whether we are making any impact on it".[28] The crimes that are recorded are usually where there has been some monetary loss. Dr Clayton recommended the "recording of all

[25] Ev 38, para 5

[26] "Cost of Cyber Crime", *Detica*, 2 February 2011 http://www.baesystemsdetica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

[27] Ev 33, para 45 [Dr Richard Clayton]

[28] Ev 30, para 10

electronic crime incidents, not just those resulting in monetary loss”.[29] SOCA appeared to agree, pointing to the US where there is “a better understanding of the threat in the US due to mandatory requirements to report data breaches in most US states. In the UK there is no obligation to disclose, and estimates of the costs of malware are difficult to assess”.[30]

22. In the *Cyber Security Strategy*[31] the Government announced that it would seek to enhance the ability of the public to report cyber crime. The Government also mentioned the possibility of developing a cyber hub with the aim of increasing the sharing of information among businesses. However, the report does not indicate whether this would involve reporting cyber crime that targeted businesses.

23. **We welcome the Government’s commitment in the *Cyber Security Strategy* to enhance the ability of the public to report cyber crime. We recommend that the Government consider how to encourage (or require) businesses to report incidence of cyber crime. Additionally, we urge internet security companies to work with Government to find a way to use the development of a cyber hub to facilitate the detection of malware.**

24. One of the problems for internet users is that much of the information about internet technology and security issues is laden with jargon. It may be difficult to get people to engage with information on security concerns when the language used to describe the dangers acts as a barrier to that engagement. As the Minister said:

> in some ways we wrap a lot of this information up in technology-speak, which sometimes makes it a little bit impenetrable for the public and others to have a sense that it is directly relevant to them. The communications strategy must have that idea at its heart.[32]
>
> […]
>
> it can at times sound as if you are talking through a complicated plot from a science fiction novel, whereas in fact, what we are talking about is real-life crime and real-life impact.[33]

25. Janet Williams, the Deputy Assistant Commissioner of the Metropolitan Police told us

> we all understand that we won’t walk down a dark alley in preference to a lit alley. That is instinctive, and we almost need to get to that point with this, so that people understand what the danger signs are, and at the moment most people don’t.[34]

To those in the know, it may seem impossible to believe that people are still taken in by the Nigerian 419 scams[35] or related ones involving winning sums of money on international

[29] Ev 30, para 10

[30] Ev 40, para 14

[31] Cabinet Office, *Cyber Security Strategy*, 25 November 2011

[32] Q60

[33] Q61

[34] Q55

lotteries.[36] It is true that there are any number of websites such as scambusters.com or snopes.com where it is possible to find the truth behind scams on the internet. However, those new to the online environment may not have sufficient knowledge and awareness and there is no obvious central point for them to consult. However, it is arguably easier to teach the public about scams as these are often simply the same types of confidence tricks that existed prior to the internet but are now using new technology to reach a new audience or to provide enough misdirection to evade the awareness people may have about physical junk mail offerings.

26. Infection with malware, on the other hand, takes cyber crime apparently to a different level—where experts use their technical skills to, among other things, take over computers worldwide to steal bank details and identity information. Dr Richard Clayton did not believe it was possible to bring the mass of the population up to the level of technical knowledge required to defend themselves; instead we needed to "rely on those who make the software to adapt it in such a way that you no longer need to read the URL[37] in order to be safe".[38]

27. If people are reluctant to go online because of fears about safety then they may find themselves disadvantaged in terms of retail opportunities and, more importantly, in terms of access to government information, advice and other services.

28. **Knowledge is the best defence against fear and we recommend that government-provided information focuses on how to be safe online rather than warns about the dangers of cyber crime. We also recommend that the Government work with the industry partners announced in the *Cyber Security Strategy* to promote the equivalent of a 'Plain English' campaign to make the technology easier to understand and use.**

Smartphones

29. Viruses and other malware were not, until recently, a problem for phone users. However, there has been a significant rise in the number of people in the UK using smartphones to access material not simply through the phone networks but also through the internet via wi-fi connections.[39] Research in Motion brought to our attention research by Gartner that suggested that smartphones will outnumber PCs by 2013.[40] PhonepayPlus highlighted to us that there was a growing threat to consumers from potentially harmful applications for mobile phones and a growing need to create awareness among consumers and industry of new threats in the digital sphere.[41]

[35] A scam where an email purports to be from officials from troubled nations seeking help to move large sums of money to the UK. Helpers are promised large rewards for their help but are instead tricked into providing upfront money or bank account details.

[36] For examples see: "Advance fee fraud", *Wikipedia*, en.wikipedia.org/wiki/Advance-fee_fraud

[37] URL is the internet address of a website such as www.parliament.uk – this may reveal a different destination to the one that the user thought they were going to by following a link in an email or website.

[38] Q10 [Dr Clayton]

[39] "A nation addicted to smartphones", *Ofcom*, August 2011, stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr11/

[40] Ev w41, para 2

[41] Ev w39, para 2

30. Our witnesses raised the point that there is a significant generational difference in how people approach online concerns.

> The older generation, which may not have used computers regularly, are now starting to use them and have a lack of technical awareness but perhaps have a different view of security. The younger generation is possibly quite the opposite, having far more experience of technology but perhaps being less aware of the need to be secure.[42]

31. **We recommend that the Government take note of the importance of addressing different messages to different generational groups of UK internet users.**

32. We were told by Mr Emms and Professor Furnell, in their joint submission from Kaspersky and the University of Plymouth, that there is some concern that computer users do not apply their awareness of the dangers of malware to mobile phones.

> Ofcom now suggests that [while] approximately one in three UK adults use a smartphone there is a distinct lack of understanding around related security issues—a recent report from Retrevo suggests that only a third of Android users are aware that their devices could be susceptible to malware, while Lookout reports an 85% increase in mobile malware detections on the Android platform during the first six months of 2011, along with a five-fold increase in the number of malware-infected apps.[43]

As increasing levels of online activity once confined to desktop and laptop computers takes place on smartphones, PhonepayPlus consider that there is a role for regulation[44] similar to that for premium services on mobile phones. However, regulation of online activity would have to apply to both smartphones and traditional internet platforms (desktop and laptop computers) and Dr Clayton suggested that consumer expectations of the platforms were different and that consumers would be less likely to accept the level of control on their computers that telephone companies exert over their mobile phones.[45]

33. PhonepayPlus, the UK regulator of premium rate services, also told us that premium rate services in the UK are worth "in excess of £800m annually" and that the movement of the market can be so rapid that the consequences of changes could be beyond most consumers' ability to grasp.[46] They raised concern about whether the regulatory framework that has worked to protect consumers in relation to premium rate services was sufficient to regulate new online services that involve micropayments.[47] A recent estimate puts the global growth in micropayments from $320 billion to $680 billion by 2016.[48]

[42] Q6 [Dr Westmacott]

[43] Ev w9, para 24

[44] Ev w40, para 13

[45] Q25 [Richard Clayton]

[46] Ev w41, para 21

[47] Micropayments are online transactions that are of small denominations e.g. $2, £3.50, or €4, and can be used for digital content purchase such as games, music, movies, comics and electronic books. Micropayments can also be used to charge for digital services such as Facebook applications and access to website member areas.

[48] The Advanced Payments Report 2011, Edgar, Dunn & Company, February 2011

34. The *Cyber Security Strategy*[49] mentioned smartphones only to point out the increasing targeting of this platform by malware but said nothing about exploiting synergies. **We are impressed by PhonepayPlus' expertise on the dangers of criminal exploitation of smartphones. We recommend that PhonepayPlus has a dedicated part of the enhanced Get Safe Online website and that they are consulted closely in the development of regulatory policy to take into account, for example, online services involving micropayments.**

Policing the internet

35. The internet does not have the same level of regulation as mobile phones. There is no overarching body that provides consumers with a first place of contact to complain about disreputable or criminal behaviour. It is not the responsibility of an ISP to regulate behaviour online. It is not the job of Nominet to decide what is or is not disreputable behaviour or to enforce a code of conduct on those offering commercial services online. It is not even the responsibility of Ofcom to decide who is a fit and proper person to operate as an ISP. The default for an individual who experiences cyber crime would appear to be to refer it to the police or possibly simply attempt to minimise any financial loss by contacting banks and online services, depending on the exact nature of the crime. There is no single first point of advice and help for the consumer.[50]

36. Cyber crime issues are handled by a number of police agencies and units. Although the police themselves were clear about the relevant lines of responsibility and authority between units,[51] those outside the police were confused, which suggests that work is needed to make the policing responsibilities more transparent to enable victims of crime to contact the right officers.[52]

37. **We recommend that the police have dedicated pages on Get Safe Online on which they might communicate directly with the general public, to gather information and intelligence about what is happening to individual computer users and to provide consumers with an authoritative policing voice on current cyber crime issues.**

38. While the police now clearly take the problem of cyber crime seriously, both they[53] and the Minister[54] agreed that the policing of cyber crime needed to become mainstream to the point that local police officers are comfortable talking about cyber security. We share the sentiments of Janet Williams of the Association of Chief Police Officers (ACPO):

> I don't think we are as good as we need to be in policing, in terms of every single police officer in this country being as equipped to give a member of the public a piece

[49] Cabinet Office, *Cyber Security Strategy*, 25 November 2011

[50] Q32

[51] Q46 [Janet Williams]

[52] For example, Ev 29, para 25 [Professor Sommer]

[53] Q37 [Janet Williams]

[54] Q84

> of advice around cyber-security as they are, for example, for their windows and their doors—their general house issues.[55]

39. More police officers need to have an understanding of cyber crime, at least to the point of properly recording the crime that takes place and signposting victims to relevant organisations that can provide help and advice. The Government recently published its shadow Strategic Policing Requirement,[56] which focuses on policing capability to respond to a large-scale cyber incident rather than the more workaday ability to respond generally to cyber crime. **We recommend that the Government ensures that the Strategic Policing Requirement addresses individual-level cyber crime, not least because much of it appears to be directed by organised crime gangs. Given competing local priorities for funding policing activities, only establishment within the Requirement will ensure that police forces invest the money necessary to guarantee that local officers are able to respond to individual victims of cyber crime.**

40. We remain concerned that there exists a clear gap between aspiration and action on the ground. Janet Williams[57] and the Minister[58] indicated their intent to tackle cyber crime at all levels. At the same time Charlie McMurdie, from the Metropolitan Police e-Crime Unit, said: "We could arrest 200 people tomorrow, but they may be low-level users of compromised data".[59] There is obviously a tension between the need to make criminals feel unsafe about being involved in cyber criminality and the desire to use those criminals to track back to the 'root cause—the two, three, four or half a dozen instances of top-end criminality' who direct and control the foot-soldiers.[60] However, if the police and Government want to ensure that "cyber criminals should not feel safe"[61] then they need to find a way to tackle even low-level users of compromised data.

41. One practical operational problem in relation to cyber crime is the global nature of the threat and the strictly national base of policing around the world. Janet Williams emphasised the impact that the police could make in partnership with the IT industry to tackle global concerns rather than the effectiveness of international policing agencies such as Europol and Interpol.

> Now, we work hand in glove with industry, and we are using its people and kit alongside our people and our kit, which enables us to cross jurisdictions. We know that cyber-criminals don't like this and that they are getting quite nervous about that capability. I think that is a good thing; we need more of that because it is obviously working.[62]

[55] Q31 [Janet Williams]

[56] A statement of the collective capabilities that police forces across England and Wales will be expected to have in place in order to protect the public from cross-boundary threats such as terrorism, civil emergencies, public disorder and organised crime. The shadow requirement is advisory but a statutory requirement is expected in the Summer of 2012.

[57] Q31

[58] Q84

[59] Q36 [Charlie McMurdie]

[60] Q36 [Charlie McMurdie]

[61] Q34 [Janet Williams]

[62] Q34

However, Charlie McMurdie assured us that when it came to operational activity, police internationally are working better together to tackle the issue of cyber crime:

> we have just conducted a recent operation—website suspension work, with rogue medical websites—with 80-odd countries, which was co-ordinated by the Interpol control centre. It provided capability for us and put all the various points of contact in place. But far more work is with Europol, currently. Interpol is just relocating as well, so it has been through quite a move; it is looking at bigger growth, to put in more capability.[63]

We are convinced that the Government and police are working closely together to address some of the international problems of ensuring that policing across national boundaries is more effective.

42. Janet Williams told us that the legislation for prosecuting cyber crime was 'not fit for purpose'; but was less clear as to where she believed the weaknesses lay.[64] The Minister assured us that the legislative framework was constantly under review to ensure it was fit for purpose.[65] We are not persuaded that there is a pressing need for new legislation. We agree with the Minister that any legislation that may be introduced should be technology neutral to ensure that the fast pace of technological change does not render legislation obsolete as soon as it gets onto the statute books.

43. **Both the Government and the police appear to want the response to low-level cyber crime to be a mainstream part of UK policing. Only when police officers are comfortable operating in online contexts and using existing legislation to tackle online theft and fraud will it be possible properly to identify whether additional legislation is required. However, we think it is important that those engaged in low-grade cyber crime can be punished without recourse to courts and that the Government should work hard with the industry to develop effective online sanctions for cyber criminals as indicated in the *Cyber Security Strategy*.**

44. **We welcome the commitment in the *Cyber Security Strategy* to make it easier and more intuitive for the public to report online crime. We urge the Government to ensure that this reporting function is integrated with the development of the Get Safe Online site as a one-stop shop for online security information and issues.**

Providing a service

45. One of the beneficial features of the internet is that it drives greater sharing of information. We were disappointed, therefore, to learn that ISPs might fail to share information with their users. Dr Richard Clayton told us:

> when a botnet is shut down it is now usual practice to set up a 'sinkhole' that will log the identities of the compromised machines which continue to try and make contact with the disabled [command and control server].

[63] Q48

[64] Q53

[65] Q85

> The operators of the sinkhole are unable to communicate with the owners of the compromised machines directly—they can only identify the ISP that is providing Internet connectivity. So it is up to the ISP to pass the bad news on to the relevant customer, because only the ISP knows who was using the IP address at the relevant time. In practice, very few ISPs relay information and almost none go looking for further sources of this type of data.[66]

This is in contrast to the situation in Australia:

> It is estimated that over 90 percent of Australian home internet users are customers of the 82 ISPs participating in the [Australian Internet Security Initiative] (ACMA, 2011). When these ISPs have been informed by the [Australian Communications and Media Authority] that a customer's computer has been infected with botware they can select from a range of responses as set out in the voluntary icode. These options include:
>
> (a) contacting the customer directly (by phone, email or SMS or other means);
>
> (b) regenerating the customer's account password to prompt customers to call the helpdesk so they can be directed to resources to assist;
>
> (c) applying an 'abuse' plan where the customer's Internet service is speed throttled;
>
> (d) temporarily quarantining the customer's service, for example by holding them within a 'walled garden' with links to relevant resources that will assist them until they are able to restore the security of their machine;
>
> (e) in the case of spam sources, applying restrictions to outbound email (simple mail transfer protocol –SMTP); and/or
>
> (f) such other measures as determined by the ISP consistent with their terms of service (Internet Industry Association, 2010).[67]

46. In the UK, there is no such driver for ISPs to intervene on behalf of their users. Dr Clayton told us that there are good and bad companies.

> We can see how poor the data passing is by examining the data collected by the Shadowserver Foundation, who operate a sinkhole for Conficker—malware that infected 7 million machines worldwide in November 2008 and which still poses a threat to the infected machines. The Shadowserver data shows that infections have dropped from 5.5 million in September 2010 to 3.5 million now; the worst affected UK ISP has seen a reduction from 7000 to 5000 infected machines over the same period. The best ISPs completely eradicated the problem, and ensured their customers were safe, two years or more ago...[68]

[66] Ev 32, paras 31 and 32

[67] Ev w38, paras 15 & 16

[68] Ev 32, para 33

47. **We recommend that the Government work with ISPs to establish an online database where users can determine whether their machine has been infected with botware and gain information on how to clean the infection from their machine. We think that this should also be integrated with the Get Safe Online website.**

3 Defences against cyber crime

48. From the evidence we have received it is clear that there is no easy technological answer to cyber crime. We have also been told that hardware solutions are likely to unduly restrict computer users in their activities while software solutions require constant updating and a more advanced understanding of the technology to be truly effective. Initiatives such as digital identities could improve general security but unless there was a way of ensuring that those identities could be used universally across applications and services this would not make life easier for users of the internet. In fact, such an approach has a single point of failure, which could lead to a single security breach with a greater impact on the user.[69] Determined criminals will circumvent the strongest automatic defences.

49. The Government 'digital by default' policy will increasingly require those in receipt of Government benefits and services to access these online. We are concerned that this policy may increase the number of users without the means to afford the best equipment or anti-virus software online or the level of knowledge to understand what is necessary to remain secure. We accept that the Government's digital identity assurance scheme, as outlined in the Minister's supplementary evidence, is designed to provide security in accessing those services. However, we also have concerns that the scheme will be of greater use in protecting the Government against welfare fraud than the individual user against crime.

50. For individual computer users, cyber crime is most likely to occur through casual infections and unfortunate happenstance. We have been told that the best defence against this kind of crime is more knowledgeable computer users[70] and that 80% of protection against cyber-attack is routine IT hygiene.[71]

> There is a balance to be struck in terms of encouraging technology usage without engendering over-reliance upon it. While users should be expected to have protection, they should not be lulled into a false belief that it will solve all their problems. Technology needs to be understood in the wider context of safe online behaviour.[72]

51. One problem is that the technology is being approached as just another consumer appliance 'like a video machine or a Skybox' which comes with 'a series of services'.[73] There is little interest among consumers in how computers work or in understanding the principles of how those computers connect with the internet.[74]

52. That lack of interest is reflected in poor awareness of personal online security:

> findings from a 2007 survey of 378 US homes by McAfee and National Cyber Security Alliance (in which users were asked about the safeguards they believed were

[69] Q16

[70] Q6

[71] Q10 [Professor Sommer]

[72] Ev w10, para 34

[73] Q4 [Professor Sommer]

[74] As above

> on their PCs, and the systems were then scanned to check the reality) revealed that while 92% believed their antivirus was up-to-date, only 51% had [updated their database] within the previous week.[75]

Meeting the need for better products and services

53. Information submitted to us by Kaspersky and the University of Plymouth also indicated that, even when security products were installed, those products are often not easy to use without more technical knowledge than the average computer user might be expected to possess:

> as illustrated by these quotes from end-users interviewed in a Plymouth University study[76]: [1] "The antivirus programs are really difficult to use, annoying because you try to access something and you get too many pop up messages, they drive you crazy, with warnings and warnings and allow or not allow"; [2] "I feel now annoyed because of the problems that (AV software) caused me. I'm a bit worried because when my laptop gets stuck my mind goes straight away maybe it's a virus, maybe it's a Trojan horse, maybe it's a worm, you know, and then I don't know what to do and sometimes I feel insecure".[77]

54. Furthermore, internet security products struggle to keep up with the development of malware. Dr Richard Clayton monitored the performance of internet security software against a new malware variant:

> It was tested at 16:54 (90 minutes after the criminals stopped deploying it) and by that time it was detected by only seven of 44 anti-virus products; and those seven did not include any of the top three products by market share. Even 24 hours later, only 11 products reported this particular malware sample to be bad.[78]

Given the enormous number of users online, a window of twenty-four hours in updating internet security software potentially exposes a huge number of users to infection by malware.

55. Stop Badware proposed a number of ways in which the computer industry could supplement standard security software and improve consumer knowledge:

- Web hosting providers could help protect customers' websites from becoming compromised by malware.
- Software vendors could design sensible security defaults and automatic update mechanisms into operating systems and applications.
- Technology industry players could collaborate on common messaging and security standards to reduce end user confusion.

[75] Ev w9, para 23 [David Emm and Professor Steven Furnell]

[76] Furnell, S., Tsaganidi, V. and Phippen, A. 2008. "Security beliefs and barriers for novice Internet users", Computers & Security, vol. 27, no. 7–8, pp235–240.

[77] Ev w9–10, para 26

[78] Ev 31, para 26

- ISPs could notify customers whose devices exhibit malware behaviour and direct those customers to educational content and support resources.[79]

56. We note the commitments made in the *Cyber Security Strategy* that the Government will work, in partnership with industry, to improve consumer awareness. However, we also note that the Stop Badware recommendations would require a higher level of co-operation between various parts of the IT industry than is evident in the Strategy. The growing incidence of malware and the fact that a very high proportion of the population are online provides scope for fraud and theft on a massive scale. Just as vehicle manufacturers have been required to treat vehicle security more seriously in recent years with a huge impact on the incidence of theft of and from vehicles, there is no reason why the IT industry should not shoulder greater responsibility for the security of its property. This does not reduce the need for individuals to be properly informed so that they have greater understanding and control over the risks they face. There needs to be a partnership between industry and customer.

57. **It would be possible to impose statutory safety standards on software sold within the EU, similar to those imposed on vehicle manufacturers, but we would prefer a solution based on self-regulation. However, the industry must demonstrate that any proposed solution would be an effective way forward and that voluntary commitments would provide sufficient incentive for the industry to improve security in a fast-moving competitive marketplace. In the event that the industry cannot demonstrate an effective self-regulatory model, we recommend that the Government investigate the potential for imposing statutory safety standards.**

Better informed consumer

58. The internet is not lacking in information for computer users about internet security. However, much of that information is technical or jargon-filled. It is hard to identify reliable information and some information may actually be provided by malware producers seeking to infect more computers. Even among reputable websites there is a lack of co-ordination: Richard Clayton told us that there was ‘a wide range of websites, and, if you collect all of their top 10 tips, you can get a list of 100 or more good things you should do. It shows how complicated this area is’.[80]

59. One resource that has been repeatedly suggested has been the Get Safe Online website. However, there was a consensus among our witnesses that the general awareness of computer users about this resource could be better. Professor Sommer highlighted the problems faced by the website:

> The trouble is that it is not well resourced; it is a bit of a gesture. It is run by a former police officer whom I have known for years. But it is a virtual organisation, with no premises, and it does not have people permanently in London ready to produce

[79] Ev w12, para 10

[80] Q6

> instant comments for the press because the website is generic and does not necessarily always reflect the latest range of risks.[81]

60. Written evidence from the Home Office gave us an insight into how the Government intended to improve public awareness:

> Much has been done to raise awareness of online threats, including through the website Get Safe Online. We will build on that initiative and others by developing a single Government portal for the provision of advice on internet safety to the public and businesses. We will ensure that the information gathered by law enforcement and the private sector which might help internet users is shared. We will drive this by making sure that every Government website, as well as DirectGov, contains a link to this safety information.[82]

The Minister indicated that this would be achieved through an upgrading of the Get Safe Online site rather than the establishment of a new site.[83]

61. **We recommend that the Government invest in the Get Safe Online site to ensure that it integrates all of the relevant organisations necessary to provide a single authoritative source on which computer users could rely. We also recommend a prolonged public awareness campaign to raise awareness of the issue of personal online security and the presence of the website to achieve the best possible information level among all computer users.**

62. **We agree with the Government that effort is needed to raise awareness of the advice available on the get Safe Online website. We expect the joint action plan mentioned in the *Cyber Security Strategy* to provide details of what will be done to raise awareness. Moreover, the Government should persuade private industry to cross promote Get Safe Online. Television exposure is crucial to gain the widest possible exposure to the safety message. We also recommend that all government websites should point towards Get Safe Online and feature security updates from the Get Safe Online website.**

63. During our oral evidence it became apparent to us that there was a simple mechanism that could be put in place relatively quickly and easily.[84] The threat of malware and cyber crime is intrinsically linked to the acquisition of electronic goods that permit access to the internet. At this point of contact between retailer and consumer there is an opportunity to provide information on the dangers of the internet and the basic precautions that should be taken to avoid them.

64. The Minister indicated that he would be willing to discuss, with business, efficient and effective ways of providing consumers with advice on internet safety.[85] Brick and mortar shops should be able to provide hardcopies of this advice while confirmation emails for online sales could be accompanied by a direct link to online advice. **We recommend that**

[81] Q6

[82] Ev 25, para 37

[83] Q66; see also Cabinet Office, *Cyber Security Strategy*, 25 November 2011

[84] Q56

[85] Q63

the Government require that access to Get Safe Online advice is provided, by vendors, with every device capable of accessing the internet.

65. Any victim of cyber crime should be able to work through the site to find the relevant authorities or trusted service providers and information they need to address the problems caused by malware and to understand what needs to be done to remedy their situation. Action Fraud, PhonepayPlus, the police e-crime unit and so on should integrate information to improve cross-fertilisation and help ensure that users do not need to understand which organisation is relevant to their problem to gain the information and assistance they require.

66. The purchase of computers and other technology that can access the internet is rarely accompanied by information about how to remain safe online. The purchase of services from an internet service provider (ISP) is more often accompanied by a description of the delights that the internet could provide rather than a list of the housekeeping necessary to maintain personal security when online. The purchase of software is more likely to be guided by features and price rather than any consideration of how secure the product might be.

67. We agree with the Government's aim of providing more information to the public and small businesses that might aid them in making informed decisions about hardware, software and services that lead to more secure online experiences. One option mentioned by the Minister was to launch a kitemark for such products, to indicate that they met specific security criteria.[86] However, accreditation of products and services usually require producers to pay for the analysis and awarding of that accreditation and we have concerns that kitemarks may simply lead to the most expensive software having a kitemark and smaller software houses making a business decision to avoid the costs. This would leave the consumer with a choice between expensive assured software and a range of more affordable but undifferentiated products. **We recommend the Government look to investigate the potential for solutions that will lead to a less clear cut division of the market by allowing lower up front costs for smaller software developers and a range of security standards.**

68. Any kitemark and accreditation solution begs the question of who should be responsible for awarding that kitemark. There is a wealth of expertise available both within the Government and the private sector with regard to the security testing of software. GCHQ is a central plank in the Government's *Cyber Security Strategy*. The written evidence to the Committee from technology companies would indicate that there is a readiness among the industry to contribute to solutions to malware and cyber crime issues. Get Safe Online is a collaborative effort between Government and the industry to improve the awareness of computer users and may provide a template for collaborative work of this nature.

69. We consider it likely that the ability and resource to produce an online testing system already exists and that such an automated system would provide an efficient method of testing software and detecting security flaws.

[86] Q79

70. **We judge that there will be a need for an automated way to assess the security of software, even if simply to provide smaller companies with a means of testing and redesigning their software prior to spending money on kitemarks. We recommend that the Government explore whether this might best be developed by Government, for Government, in partnership with private industry or by entirely private concerns.**

A healthier online community

71. We asked the question, in our call for evidence, whether the Government had a public health style responsibility to ensure the relative health of UK machines. Many of the submissions did not think that the analogy between public health and infection by computer viruses was a good fit. However, Microsoft believed that there was some value in the analogy as it prompted consideration of several important functions common to both.

> First, we should strive for a trusted system with clear roles and responsibilities just like we have for doctors, paramedics and epidemiologists in human health. Second, computer users need to know who and where to get help with a malware issue. Just as individuals can recognize a hospital or pharmacy, it must be clear to them who can be trusted to provide assistance with malware prevention and remediation. Prevention or wellness is another topic that should be adopted from human health. To do so, we must begin with an understanding of what it takes to keep a system healthy and develop the social and technical norms to encourage the healthy state of all devices. Finally, as with epidemic preparedness, industry and government must be prepared for a potential malware outbreak in a way that leverages the trusted system and roles outlined above.[87]

72. The Government took a similar perspective:

> In this respect, the approach we are taking to combating malware is similar to how the Government approaches the control of human disease, being a multi-stakeholder approach which looks at the problem holistically, resulting in a number of policy options to tackle the creation and distribution of malware in parallel to mitigating the damage caused and bolstering defences. In addition, in some circumstances infected systems may also be quarantined.[88]

73. We are inclined to agree that there is a moral imperative for the Government and industry to support consumers in being safe and secure online. Both the industry and the Government have clear interests in greater use of technology and the internet. This interest should not be served through decreased security of consumers and the users of those services. The public need clear identification of trusted information sources and relevant authorities and clear guidelines on how to help themselves stay free of infection.

74. **The Government is clear that many government services will move to online provision either directly or through a range of providers. It is also clear that an increasing proportion of UK economic activity will be conducted through or related to the internet. We ask the Government to provide, in response to this report, details of**

[87] Ev w33, para 5.2

[88] Ev 26, para 38

how they intend to engender greater trust in online products and services within the UK population and an assurance that online by default will mean better and more secure, rather than merely cheaper, government services.

Conclusions and recommendations

The importance of trusted information

1. The Government is clear that many government services will move to online provision either directly or through a range of providers. It is also clear that an increasing proportion of UK economic activity will be conducted through or related to the internet. We ask the Government to provide, in response to this report, details of how they intend to engender greater trust in online products and services within the UK population and an assurance that online by default will mean better and more secure, rather than merely cheaper, government services. (Paragraph 74)

2. We welcome the Government's commitment in the *Cyber Security Strategy* to enhance the ability of the public to report cyber crime. We recommend that the Government consider how to encourage (or require) businesses to report incidence of cyber crime. Additionally, we urge internet security companies to work with Government to find a way to use the development of a cyber hub to facilitate the detection of malware. (Paragraph 23)

3. Knowledge is the best defence against fear and we recommend that government-provided information focuses on how to be safe online rather than warns about the dangers of cyber crime. We also recommend that the Government work with the industry partners announced in the *Cyber Security Strategy* to promote the equivalent of a 'Plain English' campaign to make the technology easier to understand and use. (Paragraph 28)

4. We recommend that the Government take note of the importance of addressing different messages to different generational groups of UK internet users. (Paragraph 31)

5. We recommend that the Government invest in the Get Safe Online site to ensure that it integrates all of the relevant organisations necessary to provide a single authoritative source on which computer users could rely. We also recommend a prolonged public awareness campaign to raise awareness of the issue of personal online security and the presence of the website to achieve the best possible information level among all computer users. (Paragraph 61)

6. We agree with the Government that effort is needed to raise awareness of the advice available on the get Safe Online website. We expect the joint action plan mentioned in the *Cyber Security Strategy* to provide details of what will be done to raise awareness. Moreover, the Government should persuade private industry to cross promote Get Safe Online. Television exposure is crucial to gain the widest possible exposure to the safety message. We also recommend that all government websites should point towards Get Safe Online and feature security updates from the Get Safe Online website. (Paragraph 62)

7. We recommend that the Government require that access to Get Safe Online advice is provided, by vendors, with every device capable of accessing the internet. (Paragraph 64)

The need for standards

8. We recommend that the Government work with ISPs to establish an online database where users can determine whether their machine has been infected with botware and gain information on how to clean the infection from their machine. We think that this should also be integrated with the Get Safe Online website. (Paragraph 47)

9. It would be possible to impose statutory safety standards on software sold within the EU, similar to those imposed on vehicle manufacturers, but we would prefer a solution based on self-regulation. However, the industry must demonstrate that any proposed solution would be an effective way forward and that voluntary commitments would provide sufficient incentive for the industry to improve security in a fast-moving competitive marketplace. In the event that the industry cannot demonstrate an effective self-regulatory model, we recommend that the Government investigate the potential for imposing statutory safety standards. (Paragraph 57)

10. In relation to kitemarks, we recommend the Government look to investigate the potential for solutions that will lead to a less clear cut division of the market by allowing lower up front costs for smaller software developers and a range of security standards. (Paragraph 67)

11. We judge that there will be a need for an automated way to assess the security of software, even if simply to provide smaller companies with a means of testing and redesigning their software prior to spending money on kitemarks. We recommend that the Government explore whether this might best be developed by Government, for Government, in partnership with private industry or by entirely private concerns. (Paragraph 70)

Expertise and policing

12. We are impressed by PhonepayPlus' expertise on the dangers of criminal exploitation of smartphones. We recommend that PhonepayPlus has a dedicated part of the enhanced Get Safe Online website and that they are consulted closely in the development of regulatory policy to take into account, for example, online services involving micropayments. (Paragraph 34)

13. We recommend that the police have dedicated pages on Get Safe Online on which they might communicate directly with the general public, to gather information and intelligence about what is happening to individual computer users and to provide consumers with an authoritative policing voice on current cyber crime issues. (Paragraph 37)

14. We recommend that the Government ensures that the Strategic Policing Requirement addresses individual-level cyber crime, not least because much of it appears to be directed by organised crime gangs. Given competing local priorities for funding policing activities, only establishment within the Requirement will ensure that police forces invest the money necessary to guarantee that local officers are able to respond to individual victims of cyber crime. (Paragraph 39)

15. Both the Government and the police appear to want the response to low-level cyber crime to be a mainstream part of UK policing. Only when police officers are comfortable operating in online contexts and using existing legislation to tackle online theft and fraud will it be possible properly to identify whether additional legislation is required. However, we think it is important that those engaged in low-grade cyber crime can be punished without recourse to courts and that the Government should work hard with the industry to develop effective online sanctions for cyber criminals as indicated in the *Cyber Security Strategy*. (Paragraph 43)

16. We welcome the commitment in the *Cyber Security Strategy* to make it easier and more intuitive for the public to report online crime. We urge the Government to ensure that this reporting function is integrated with the development of the Get Safe Online site as a one-stop shop for online security information and issues. (Paragraph 44)

Formal Minutes

Wednesday 25 January 2012

Members present:

Andrew Miller, in the Chair

Stephen Mosley	Graham Stringer
Pamela Nash	Roger Williams

Draft Report (*Malware and cyber 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 74 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Twelfth 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 placing in the Library and Parliamentary Archives.

[Adjourned till Wednesday 1 February at 9.00 am

Witnesses

List of printed written evidence

List of additional written evidence

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

1	Dr Huma Shah (Malware 02)	Ev w1
2	David Emm and Professor Steven Furnell (Malware 03)	Ev w7
3	StopBadware (Malware 05)	Ev w11
4	Finmeccanica Cyber Solutions (Malware 06)	Ev w13
5	Messaging Anti-Abuse Working Group (MAAWG) (Malware 07)	Ev w14
6	McAfee (Malware 08)	Ev w18
7	Symantec (Malware 09)	Ev w22
8	Amit Bhagwat (Malware 12)	Ev w25
9	Raytheon UK (Malware 15)	Ev w27
10	Dellsecureworks (Malware 16)	Ev w29
11	Microsoft (Malware 17)	Ev w31
12	Australian Institute of Criminology (Malware 19)	Ev w34
13	PhonepayPlus (Malware 20)	Ev w39
14	Research In Motion (Malware 21)	Ev w41

List of Reports from the Committee during the current Parliament

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2010–12

First Special Report	The Legacy Report: Government Response to the Committee's Ninth Report of Session 2009–10	HC 370
First Report	The Reviews into the University of East Anglia's Climatic Research Unit's E-mails	HC 444 (HC 496)
Second Report	Technology and Innovation Centres	HC 618 (HC 1041)
Third Report	Scientific advice and evidence in emergencies	HC 498 (HC 1042 and HC 1139)
Second Special Report	The Reviews into the University of East Anglia's Climatic Research Unit's E-mails: Government Response to the Committee's First Report of Session 2010–12	HC 496
Fourth Report	Astronomy and Particle Physics	HC 806 (HC 1425)
Fifth Report	Strategically important metals	HC 726 (HC 1479)
Third Special Report	Technology and Innovation Centres: Government Response to the Committee's Second Report of Session 2010–12	HC 1041
Fourth Special Report	Scientific advice and evidence in emergencies: Government Response to the Committee's Third Report of Session 2010–12	HC 1042
Sixth Report	UK Centre for Medical Research and Innovation (UKCMRI)	HC 727 (HC 1475)
Fifth Special Report	Bioengineering: Government Response to the Committee's Seventh Report of 2009–10	HC 1138
Sixth Special Report	Scientific advice and evidence in emergencies: Supplementary Government Response to the Committee's Third Report of Session 2010–12	HC 1139
Seventh Report	The Forensic Science Service	HC 855 (Cm 8215)
Seventh Special Report	Astronomy and Particle Physics: Government and Science and Technology Facilities Council Response to the Committee's Fourth Report of Session 2010–12	HC 1425
Eighth Report	Peer review in scientific publications	HC 856 (HC 1535)
Eighth Special Report	UK Centre for Medical Research and Innovation (UKCMRI): Government Response to the Committee's Sixth Report of session 2010–12	HC 1475
Ninth Report	Practical experiments in school science lessons and science field trips	HC 1060–I (HC 1655)
Ninth Special Report	Strategically important metals: Government Response to the Committee's Fifth Report of Session 2010–12	HC 1479
Tenth Special Report	Peer review in scientific publications: Government and Research Councils UK Responses to the	HC 1535

	Committee’s Eighth Report of Session 2010–12	
Tenth Report	Pre-appointment hearing with the Government’s preferred candidate for Chair of the Technology Strategy Board	HC 1539–I
Eleventh Special Report	Practical experiments in school science lessons and science field trips: Government and Ofqual Responses to the Committee’s Ninth Report of Session 2010–12	HC 1655
Eleventh Report	Alcohol guidelines	HC 1536

Oral evidence

Taken before the Science and Technology Committee

on Wednesday 9 November 2011

Members present:

Andrew Miller (Chair)

Stephen Metcalfe
Stephen Mosley
Pamela Nash
Graham Stringer
Roger Williams

Examination of Witnesses

Witnesses: **Dr Richard Clayton**, Senior Research Assistant, University of Cambridge, **Professor Peter Sommer**, Visiting Professor in the Department of Management, London School of Economics, and **Dr Michael Westmacott**, BCS, The Chartered Institute for IT, but also representing the Royal Academy of Engineering and the Institution of Engineering and Technology, gave evidence.

Q1 Chair: Welcome, gentlemen, to the session. Dr Clayton, I thank you for advising us previously, but today you are here formally as a witness. For the record, would you all kindly introduce yourselves?

Dr Clayton: I am Dr Richard Clayton. I am a security researcher at the University of Cambridge and the National Physical Laboratory.

Professor Sommer: I am Professor Peter Sommer, from the London School of Economics and the Open university.

Dr Westmacott: I am Michael Westmacott; I am a security consultant and also a member of BCS.

Q2 Chair: In their written evidence, the Government define malware as software written with malicious intent. Is that a useful definition, or do you have a better one?

Dr Clayton: It is a useful definition. We used to call things viruses, worms or Trojans and all sorts of other technical terms that were to do with the way in which they spread. In practice, however, most sorts of malicious software can be delivered in a number of ways, and precisely how they propagate has become less important than what they do to people. The term "malware" has grown up and become a much more mainstream way of generally indicating what is going on.

Professor Sommer: I concur. There are bigger problems in defining the cyber-crime aspect of your investigation, but the malware description given by Richard is just fine.

Dr Westmacott: Absolutely. In fact, I believe that the original definition "malicious software" applies.

Q3 Chair: I was listening to a radio interview with Ross Anderson just before last week's summit, and he argued that the problem in this area is, to use his phrase, that it's no good shooting a few alligators; you have got to drain the swamp. In other words, you have to address the whole spectrum of potential causes and the various players in the field who all have different intent. If the Government want to make substantial progress in a short period, where should they concentrate their efforts? Should it be on individual users, on ISPs or just dealing with the law enforcement side? Where would you concentrate your resources?

Professor Sommer: Are you talking about the resources of the Committee in carrying out its investigation, or the resources of the nation?

Chair: The resources of the nation.

Professor Sommer: Malware is a convenient description of things that behave badly, but they can be used for a very wide range of purposes. Perhaps you need to look at the spectrum of circumstances and make a refinement from that, but there are many different actions. Ross's phrase about it being a swamp, I suppose, is correct, but that is partly the problem with this wider phrase "cyber-crime". We should bear it in mind that three quarters of the population now has at least one personal computer in the home permanently connected to the internet. Very large numbers of activities that would previously have been called conventional crime now have some sort of cyber element. Perhaps one needs to look at the difficulty that businesses and members of the public have in understanding the nature of the new threats. That would probably be rather more useful, although there are individual sectoral aspects that one would have to look at as well.

Dr Westmacott: I believe that we need to be able to define where malware sits within crime and to look at the different types of actors involved in it. In our responses, all three of us have started to examine some of them. We also need to understand better who are the specific targets of malware. There is a lack of appreciation of exactly what types of targets there are; it could be individual members of the public, or organisations and certain aspects of Government. Once this is completed, we can start to understand where malware is generally moving toward from its current position.

Dr Clayton: A range of things needs to be done. There are two key areas. The first is that there has to be more policing, and more policing worldwide, because the people deploying the malware and doing the cyber-crime basically feel that they are not likely to get caught. Essentially, they are correct. We, therefore, have to change the balance so that there is a higher likelihood of them getting caught. That means spending more money on police and training, and having more cross-border co-operation in order to investigate these crimes.

The other thing that we can do, which we are doing very badly at the moment, is that, when individual machines are caught up in cyber-crime, as part of a botnet or whatever, people in the community should be aware of that and pass the information on to the ISPs. The best ISPs pass that information on to their users and tell them that they have a problem. But, on many occasions, the ISPs throw those reports away; they certainly do not go out seeking more reports because it is very expensive for them to communicate with their users—particularly if it is quite a complicated message to put across—to tell them that they have a problem and that they will have to spend some money to sort out their machines. They do not like being the bearer of bad news.

Professor Sommer: There is also a wider dimension. If you look at the things that make cyber-crime possible, one of the other aspects of it is what is called social engineering. People are taking advantage of the fact that many members of the public do not have an inbuilt detector that allows them to recognise that things coming up on their computers may be fraudulent. In fact, many cyber-crimes, as they occur in the real world, show a combination of social engineering and malware. Part of the general problem is the rate of change. People have got used to the idea of detecting regular crime, but the astonishing rate of change in computers, and the social, economic and cultural environments that they generate, means that they have not had a long period of learning to spot what is bad. That is the really big problem. Richard espouses the need for more policing. I do not disagree with him, but one of the areas I hope that you will be looking at is the role of education and how far the nation should be spending money on various forms of education to help people not to become victims.

Q4 Chair: In the meantime, because of the risk to individuals, organisations and, indeed, to the nation state, Dr Clayton's point about policing is relevant, and what you said about education, Professor Sommer, is clearly relevant. We need people with your skills to look over our shoulders to ensure that we do not make silly mistakes. There are bound to be tensions in this area between security and freedom. Is that inevitable and will internet users inevitably have to see their freedoms diminished to enable them to be more protected?

Dr Westmacott: Are you possibly talking about the automated monitoring of ISPs of individuals' broadband connections to see whether their systems are being infected, or whether they are browsing websites that are known to be of ill repute? Is that the sort of invasion of privacy that you mean?

Chair: Indeed.

Dr Westmacott: This argument has been made a number of times.

Professor Sommer: Indeed. I should think that at least three quarters of the speeches that I heard during my visit to the London conference on cyberspace last week were along the lines of "a balance must be struck", without a great deal of explanation of how to strike that balance. The dilemma really is this. Many people are not terribly interested in computers. They have computers in their homes, but they think that the computer is just another appliance; it is like a video machine or a Skybox or whatever and a series of services comes along.

The great advantage of the computer is that it is almost infinitely programmable to do all sorts of things; the same box that you use for your e-mails and your social networking can also be used for designing and developing complex programmes and so on. In a sense, there is a great benefit from having that very open structure, because it gives innovation not only technically but socially, culturally and economically. But that very openness means that nasty stuff can come in as well as the good stuff. It is easy to make rude remarks about people who say that a balance must be struck and who are not clear about it; but, if you said to me, "Let's hear your balance", I would not have a clear answer either. We have to recognise that it is a dilemma.

Coming back to the point about education, one of the elements of education that you have to get over to the public is that computers are not appliances. You have to spend a bit of time looking after yourself, and, although there can be help from the nation state and from policing, you have to take responsibility for it yourself.

Dr Clayton: On the privacy issue, it is possible to monitor without it being necessarily privacy-invasive. It is privacy-invasive if you monitor and keep the records for many months just in case someone from the police or Cheltenham needs to come along and have a look at them, whereas most of what we are talking about when monitoring for malware and so forth is instantaneous stuff. It is whether or not your machine is looking up a particular domain name because the malware on your machine is trying to phone home and needs to look up the domain name in order to find out where home is today. Therefore, you can monitor for activities surrounding that particular domain name without checking which particular social network you are using or which particular flavour of porn site you are going to. I would say that you do not have to record everything in order to detect the bad things.

Dr Westmacott: The technical challenges of attempting to monitor traffic for malicious activity are difficult. I operate a network forensics service, and I have to spend a lot of time manually looking through data because the automated systems in place are not sufficient. They can provide too much information and, therefore, throw up far too many false positives, or they do not provide enough information and do not identify genuine malicious activity. To place that on ISPs would be a great burden, and it is possibly a burden that they would not be able to deliver. I fully agree with Peter that education of individuals is far and away the most important factor that we need to consider.

Professor Sommer: I do not think there is a single route. It is a combination of things. You can do things as a nation state, and you can ask the ISPs or the police to do certain things. It is not a total package, and I am afraid that some of it will be down to the individual.

Q5 Chair: The tensions between individual privacy and security are very real, and we need to take them into account.
Professor Sommer: Yes, but that is true throughout law enforcement.
Chair: Absolutely.

Q6 Roger Williams: You say that, to a great extent, responsibility lies with the individual, but the individual is often the weakest link in online security. But many individuals and small organisations do not have the resources or the will to take advantage of what is there. Do you believe that sufficient information resources are accessible to the average internet user to allow them to make informed decisions about their activities and protection?
Professor Sommer: If you look across the internet for websites that are hosted in the United Kingdom, a pretty good range of advice is given, but it is all separated out and some of it may appear to be tainted. Good advice on websites is produced by the antivirus companies, but obviously they are also trying to sell you their products. Good advice is provided on the banking sites, but you get the feeling that the banks are trying to minimise their responsibilities in these areas.

There is a case for having a central Government-sponsored education facility. We have one; it is called Get Safe Online. It is having its activity week this week, as it happens. In fact, they had their meeting in a room not a million miles from where we are today. As an example of the sort of things that it could be doing, it was talking about malware on mobile phones. The trouble is that it is not well resourced; it is a bit of a gesture. It is run by a former police officer whom I have known for years. But it is a virtual organisation, with no premises, and it does not have people permanently in London ready to produce instant comments for the press because the website is generic and does not necessarily always reflect the latest range of risks.

You could say that one needs to spend more money on it. In fact, the money that is being spent could almost be wasted because below a certain level it is not likely to be as effective as it could be. It has put in a bid for part of the £650 million of real new money that has been promised for cyber-security in general, but I do not know how much of that it will be getting. We shall not know until the end of the month, when Francis Maude stands up in the House, but I would sooner see the odd million or two going from the GCHQ budget in the direction of Get Safe Online than what I fear might happen.
Dr Westmacott: Yes, the resources are there. Get Safe Online is a very good resource. Peter has just described some of the problems with the organisation itself, but there is also a problem with the public, in particular, which is a lack of awareness of security in general and a lack of understanding of the security implications there are in using computers. Further, this can be split into a generational difference. The older generation, which may not have used computers regularly, are now starting to use them and have a lack of technical awareness but perhaps have a different view of security. The younger generation is possibly quite the opposite, having far more experience of technology but perhaps being less aware of the need to be secure.

BCS recently updated its security top tips. One thing that we tried to do was to segregate it into different areas; for instance, you would be looking at tips for the elderly and vulnerable, and for the young. We need to target specific areas of the population with different types of information. In terms of Get Safe Online, there are different areas of information, but this is certainly something that could be given more attention.
Dr Clayton: There is a wide range of websites, and, if you collect all of their top 10 tips, you can get a list of 100 or more good things you should do. It shows how complicated this area is.
Professor Sommer: I did some work two or three years ago for the National Audit Office—for a variety of internal reasons it did not complete it—on a value-for-money study of the supply of Government information in this particular sector. I was asked to do the literature review. I do not represent the NAO, but I looked at the various websites that were available. As we have both said, the information is out there. However, in some ways public money is being spent on duplicated websites—it certainly was two years ago—and on partial initiatives. One rather wished that there was bit more consolidation of public funds in a central place.

Q7 Roger Williams: You seem to be putting a huge burden on individuals. Should there be an internet-user test, rather like the driving test, that you have to take before you venture into these dangerous areas?
Professor Sommer: I would be interested to hear you introducing such a law in Parliament.

Q8 Roger Williams: We are in the middle of Get Safe Online week. Have there been any surveys on the public's awareness of it?
Professor Sommer: The National Audit Office did some investigations of that, but I do not have the figures; I was merely asked to do a specific job for them. It carried out a survey, but I do not know whether it was ever published; it may have been thought to be too incomplete to put before Parliament, but the NAO did some work at the time. That is all I can tell you.

Q9 Roger Williams: Is it your feeling that awareness is not very good?
Professor Sommer: It is difficult to say. You must bear in mind how I earn my living. I am a specialist in this sort of area, and a magnet for a wide range of friends and acquaintances who come along to me with particular problems. I am probably not terribly well placed to gauge the general situation of awareness.

Q10 Chair: Picking up the point about consolidation, Get Safe Online is clearly under-resourced. It is a public-private partnership. Some big companies have bought into it, and others are talking about the possibility of joining the show. At the same time, taking Dr Clayton's point that there are plenty of resources out there, other companies are doing their own thing. Only this week, for instance, we have seen Google going to bed with the Citizens Advice Bureau. Is that beneficial, or would it be better if there was consolidation, with a much bigger thrust through a bigger public-private next-generation operation?

Professor Sommer: My own preference would be for consolidation—for a single, obvious and authoritative source on which people could rely. The question is how to organise it, given that you would still want private funding in public things. The private companies will want a bit of glory for what they do; they are not entirely public spirited. That is almost a political philosophy, but my own inclination is this. We are all agreed that the stuff is out there, but there would be a good argument for it if it was not for a huge amount. Get Safe Online does not need a gleaming skyscraper full of people, but it is probably under-resourced for delivering a useful service.

Dr Clayton: I am from a university, and I am really in favour of education. I am also in favour of training, which is different from education. There are limitations on what can be done in this area. We cannot teach the whole population to read the URL and understand what it means, but in order to understand many of the threats out there you do need to be able to read URLs. We, therefore, rely on those who make the software to adapt it in such a way that you no longer need to read the URL in order to be safe. We need a better understanding among users that the software on their machines needs constant updating in order to keep it safe, but many people are unaware of that and do not realise the significance of it.

Microsoft has gone to great efforts lately to make it very clear. If you have a modern version of Windows, you can hardly avoid seeing that it insists you update it, but that was not true until relatively recently, and it is not true of many other sorts of software. It is basically the really simple messages, such as saying that you have to update your machine. You have to pay attention to what turns up, including explanations of how some of the scams work. We would not expect anyone these days to fall for the three-card trick; how it works and the fact that you are going to lose your money is part of our culture. Equally, we need to train people on how stranded traveller or lottery scams work, so that at least halfway through they would think, "Oh, my goodness, I've been conned. I'd better stop now." That is the sort of thing that we can do, but teaching people the technical details is way beyond society's capabilities.

Professor Sommer: Two issues arise from that. The first comes back to your earlier question, Chairman, on how to balance privacy and security. One of the things that you can think about is a semi-walled garden or a safer internet. People have been talking about the possibility of internet service providers providing higher levels of security as an additional service, blocking nasty websites and so on. It has been discussed not only in this area of malware but also in connection with unpleasant material. Over the years a number of internet service providers have tried to launch such services, but because additional costs are involved they have had to charge more. As I understand it, the experience has overwhelmingly been that people will not buy it or not in sufficient quantities to make it viable. That is a real difficulty.

The second element is the rather useful statistic, which I believe is roughly correct, that was cited by Iain Lobban, the director of GCHQ. He was talking about protecting businesses from cyber-attack, but he said that about 80% of it is routine hygiene. Most of the attacks, including malware attacks, I guess, are known; there is nothing novel about them. You can assist people in protecting themselves against them because you can semi-automate it. By doing it reliably, you are at least making life more difficult for the cyber-criminal, or the more malicious cyber-attackers that he was talking about, because they will have to keep looking for more advanced techniques as the simple techniques are no longer available to them.

Q11 Pamela Nash: Dr Clayton, you spoke about trying to build up a knowledge of scams among the public, but it will be a while before we reach that critical mass on the same level as the three-card trick. But, in the meantime, the Government have said that they are developing a digital identity assurance scheme to protect against phishing scams. Do you think that this will improve on what is already available? Do you think that this could significantly contribute to the fight against malware?

Dr Clayton: Not in the slightest. That is nothing to do with it. Digital identities matter to Government because you can do better in society if you pretend to be two people—for instance, by getting two tax breaks and in all sorts of other ways. By being two people, or by being no people, you can win against the Government. Basically, industry does not care. Amazon does not care who you are; it only cares whether you can pay. In general, if you use someone else's credit card, it tends not to be Amazon that loses out, because it pays attention to where the orders are being placed, where they are being delivered, and the sort of goods being ordered. It fights crime in that sort of way, and your identity is very low on the list of things that it considers.

Professor Sommer: If you are looking at digital identity as a means of reducing the quantity of malware, you would require that digital identity system to be absolutely universal. In other words, you would not be able to go on to the internet unless you had a digital identity. You would then have to ask where that identity came from and how it was to be managed. The basis of it has to be that every single computer has somehow to be registered centrally; that central register must have a means of linking a real person to the owner of that computer; and there has to be a means of authenticating it.

You are talking about a huge infrastructure, which probably will not be economically viable. You cannot make it absolutely universal. You may be able to do that shortly after we get permanent global peace but not very much before. It is just not going to happen. As Richard said, digital identity can be useful for citizen-to-Government transactions and perhaps certain other things. Your other problem is that, if the technical system is bad or it gets compromised, then you have a single point of failure. In case you think that that is a theoretical concept, in Holland recently a company issued so-called authentication certificates to various companies that were to be used across the web but that was compromised. It is not a straightforward solution at all, I am afraid.

Q12 Pamela Nash: If there was a mandatory scheme for Government-to-citizen transactions, perhaps for banks, would it improve the security situation?

Professor Sommer: It would depend how it was implemented, but it would not deal with the vast majority of malware. I am not sure how much fraud the Government suffer across the internet in their contacts with the citizenry. If there was a particular problem of fraud or hijacked identity, it might do something, but in a sense there is already a structure, through the Government Gateway, for paying tax or whatever. There is a sort of digital identity element there. I share Richard's view. Neither of us is particularly convinced that we need a single digital identity. Identities for particular purposes are probably adequate, and they also avoid the problem of a single point of failure. If you have only one digital identity and it gets compromised, that's you finished. You will have no access to your bank or to the state, and a huge palaver in trying to rectify everything.

Q13 Stephen Mosley: I was interested in what you said earlier, Professor Sommer, about most people thinking of their computer as a consumer appliance sitting in the corner of the room. I guess that it is not only consumers in the house that do that. I imagine that most of us here today use our computers for e-mails, internet surfing, Word, and perhaps a spreadsheet or two, but that is about it. We do not use the further capabilities.

Dr Clayton said that the top 10 tips would soon roll into a top 100 tips. Do you think that we buy computers almost the wrong way around? We are buying an open box capable of all the wonderful things which you were talking about, but the reality is that most of us want that consumer appliance. When you buy a machine, should it not automatically have the highest security settings, with ports locked down and downloads blocked on the machine, rather than buying an open box that we have to configure ourselves in order to tighten security? Surely, it should be a case of getting something that is tight, and then if you want to open it up you can, but you get warnings when you do so.

Professor Sommer: There are a few answers. First, I do not know whether you remember the Amstrad PCW. It was a dedicated word processing device; that is all that it did. Actually it was a fully functional computer and you had to work quite hard to use it, but, if you did a certain number of things, you could suddenly see the operating system behind it and you could then run other sorts of programs. That was quite a good structure. There may be a good case for someone producing things along those lines.

The second issue that you raised was about security being locked down. The trouble is that the operating systems on which computers are based these days are incredibly complex and full of flaws. Although you might sell something on day one as being fully locked down, it is very likely that there will be flaws later on that can be exploited and which would make it less secure. But I do think it is an interesting idea. To a certain extent, Apple tried to follow that model with the iPhone in the sense the company made it rather difficult to put on any applications that it had not tested and specified to a certain level. To a limited extent, Apple is addressing the point. Perhaps entrepreneurs will read the minutes of this hearing and immediately produce something of the sort that you suggest.

Dr Westmacott: It was tried in the past by Amstrad; it released a phone that could perform e-mails and web-browsing, but it was not very successful. I do not know whether that was due to the implementation of the product or the fact that it restricted the computer to just two functions. One of the wonderful things about modern computers is that they can do so much, and most people buy them for those capabilities. You could restrict systems to web-browsing, but unfortunately web-browsers are now very complicated and, functionally, they perform a huge number of things. Indeed, they almost act as an operating system in their own right, and they can be updated with different software components, but those components could be vulnerable to exploitation as they may not have been well designed. I am not sure that trying to provide a consumer device that performs limited operations would work unless you followed the business model that allowed you to control everything, much as Apple tries to do, to ensure full quality control of all software and everything else. Even then, if your quality controls are not sufficient, there could still be problems.

Professor Sommer: You then get another problem, which is of monopoly or quasi-monopoly suppliers. You will get people complaining that Apple is taking too large a share of books and newspapers that are sold over too large a share of the apps, or applications, that are being run. It is a route, but, as with everything that we have been discussing today, it is only a partial solution.

Dr Clayton: It is probably very immodest of me to say so, but I wrote the code for the Amstrad PCWs and I had nothing whatsoever to do with the Amstrad phone. You can draw whatever conclusions you want from that.

It is true that Apple operates a system which is basically, "Lock everything down. Never ask a user a question. Always know the answer to it." Microsoft has produced a system that is extremely open, and, when it is not sure what to do, it asks the user an incomprehensible question and gets them to answer yes or no. That question is asked because there are generally some people in the world who will answer it in one way and some who will answer it another.

Your question is a little out of date in that, when you get a machine these days, whether from Apple, Microsoft or anyone else, it is in fact considerably locked down compared to the situation that was true many years ago. The difficulty is that it tends to come with anti-virus software on it, but it is only good for 30 days, and that is entirely unclear to people.

Therefore, after 30 days, that extremely good protection evaporates and you then have less protection. Equally, I am very cynical of the power of anti-virus software to spot many threats, so perhaps it does not make all that much difference. That is the sort of issue that needs to be considered—what things are bundled together and so forth. However, as soon as people get their computer home and go on the net, they will be invited to download more codecs, a flash driver and that sort of thing, and they are then pretty much on their own as to whether that is the right thing to do. If anything, I would like to see systems bought from the shops having a wider range of things being pre-installed, so that you do not have to spend the first few days installing them in order to view websites, because at that point people may install the proper codec rather than a dodgy one which is full of malware.

Q14 Stephen Mosley: Dr Westmacott, you mentioned flaws in software and quality control. Surely, the software suppliers have some liability here. They should be designing software that does not have these flaws. I know that in many cases they deliberately put holes in the software that can be exploited for their own use, but sometimes they can be exploited by others. Do the software providers not have some liability?
Dr Westmacott: Absolutely. I think of the case of software vendors installing what you might call back doors, but that practice is widely frowned upon and I do not believe that it happens as much in the real world as is believed. Certainly, software vendors certainly have a big responsibility to ensure that their products are developed securely. However, there is another driving force, which is the market, which says that they must continually be innovating and creating new products, and selling new services. The time that it takes to ensure that a piece of software is so securely developed and safe is far too long. In fact, software developed like that is obsolete by the time it is released to the market. The problem is that the software vendors are always trying to put out new products, and a certain level of risk is accepted. Another consideration is the type of software vendors. There are the operating system providers, and then there are the vendors who create software that sits on top of their operating system. The operating system vendors need to spend the most time ensuring that they have a reliable platform, as should other software vendors.
Professor Sommer: As you say, the problem is the commercial driver. What most people need from an operating system is probably delivered by more recent versions of Windows XP and in office applications such as Office 2000, and a few people would like some improvements, but it does not make commercial sense for companies such as Microsoft that need to produce high levels of revenue. They do that by producing exciting new features, some of which are less necessary than others. The more complex you make the system, the greater the chance of various parts failing.
The current position, in my view, is that Microsoft releases products far too early. It makes up for that by putting a great deal of effort into releasing caches and corrections; it is very dedicated about that and very good at talking to other companies about how it operates. However, that does not disguise the fact that, if you buy Windows 7, you have to accept that once a week you will get an update that probably requires you to reboot your computer. As I said in my written evidence, I cannot think of another product in history for which, during its entire life cycle, the manufacturer sends you a little package of screws or bolts or whatever and says, “Please install this to make your product a little safer.” You expect it to be safe. Governments, who are very big purchasers of software, are probably well placed to go back to the likes of Microsoft and say, “Your commercial interests and our requirements for safe computing do not altogether align.” Microsoft is very good at PR, and it is quite genuine in its support for a wide range of organisations, but that does not alter the fundamental problem that it releases products that are too complex and too untested, and then only afterwards tries to rectify them.

Q15 Stephen Mosley: You mentioned the Government. Is there anything on which the Government should be focusing in your opinion?
Professor Sommer: The Government are a large purchaser. If you think of the ability of an individual to complain to Microsoft, I am an individual and I know people at Microsoft, but, if I complain, they laugh and say, “Oh, there you go again.” This obviously applies also to large companies. Large purchasers, which include nation states, are in a position to make those points much more forcibly than individuals.

Q16 Graham Stringer: Approaching it from the other side, is it possible to make computers more secure by changing the design of the hardware so that the safety is built in from the very beginning? I am not sure whether that is a meaningful question, but I would be interested to hear your answer.
Professor Sommer: The short answer is no, not really. To come back to the question of digital identities, we periodically get the idea that the hardware—each motherboard or each computer—could contain a unique identity to be used as part of the rather elaborate system that you need in order to give digital identity. There are advantages and disadvantages to that. You then come back to the fact that the identity has to be registered to an individual and registered centrally, and so you have that very large cost. If we had more time, I could tell you of other problems that probably do not help very much.
Dr Clayton: What you may have in mind here is the concept of the trusted boot, where, in order to avoid malware getting on to your machine at such a low level, you cannot even detect it because the malware goes and fools the detector into saying, “I’m not here. I’m not the droid you are looking for.” The notion is that you have a chain of digital signatures so that each step checks that the next step is properly signed code that definitely comes from Microsoft and not a malware writer, before it starts running it. That is a fine system, in concept. Unfortunately, it means that

you cannot run a different operating system on that machine. You might want to run a copy of Linux or something like that, but Linux's development world is not set up to produce signed code in that sort of way and, therefore, you would not be able to run it on those sorts of machines. The people promoting this are really keen on it, because it means that once you have bought the machine you can only ever run Microsoft software on it. Microsoft is really keen on that, but it is not necessarily what you want. Equally, if you look at the handset market, again you do not expect to buy an Android platform and then run Apple software on it.

Perhaps in the handset market we are getting a diversity of platforms, but the bottom line is that, in the end, you cannot check every single piece of software because after a while it gets too complicated to do. You, therefore, end up having to accept more components running on your machine that can do bad things. Microsoft is already telling us that a lot of the failures—those times when everyone says that Windows crashed—were not caused by Windows but by the drivers, which are bits of software written by people in Taiwan to go with their particular hardware devices which are part of the machine. It sounds attractive, but it has a huge economic impact, whether or not you are building in monopolies and that sort of thing, and it probably does not solve the right problem.

Dr Westmacott: A good comparison to make is with that of the rail and airline industries, where software for trains and aeroplanes has to go through far more rigorous engineering. There is a lot of research into secure development and—I am looking at you because I can't think of the words.

Professor Sommer: I am not quite sure of the phrase you are looking for. One of the things that you get in safety-critical software—

Dr Westmacott: That was absolutely it.

Professor Sommer: That was the phrase that you were looking for—safety-critical software. To make it really safe, you strip down its functionality. If you are having software to run in the examples you gave, or to run a nuclear power station, where you do not want failure too often, you strip out the functionality. You make things safe by ensuring that it does only the simple but essential things. If you were prepared to tolerate an operating system without lots of pretty pictures but just simple text that you could send, and very simple documents and e-mails, there would be far less code to go wrong, and far less code would need to be tested. But that would probably not be acceptable to people any longer. Again, we come to the balance between lots of functionality and the ability to test it.

Q17 Graham Stringer: Again, looking at it from the other side, would it be sensible to have some self-regulation? For instance, when you first put your computer in, you get the top 10 safety tips, or the top 100, automatically on a video at the start, and, whether they like it or not, people would get some awareness of the hazards.

Professor Sommer: It is a good idea. Are you suggesting that there should be a Government regulation mandating vendors to provide that information?

Q18 Graham Stringer: Self-regulation should become an industry norm.

Professor Sommer: It is a function that Get Safe Online could perform and might be a valuable expenditure of public funding. It would not cost much money to generate that information and make it available. That would be a good educational programme. There are other opportunities for educational programmes, but it has to be treated like any other form of public education, such as drinking and driving or not spreading diseases and so on. You have to keep repeating it, and presenting the information sometimes when people do not expect it and at times that they can find it. But the route that you suggest seems a very good one to me.

Q19 Stephen Metcalfe: Professor Sommer, you said that the internet service providers had attempted to provide greater internet security for their customers but because they had to charge for it the take-up was low. If it was to become mandatory, if you were to make the internet service providers do that across the board to everyone, at what point in the network should it be? Should it be on the individual's personal machine, should it be at the internet service provider, or should it be at the connection with the landline—with BT or Virgin Media? Do you have a view on that?

Professor Sommer: The way that you phrased the questions perhaps identifies the range of problems. The particular difficulty about imposing any type of control is that the internet service providers can provide it only at what they call the subscriber level. In other words, they are delivering it to the box that you have in your house—the hub that connects to the outside world. Most of these devices are wireless and the multi-computer home varies; in a sense, what the individual user does is not in the control of the ISP. We come back all the time to the filtering problem that Richard spoke about and you were talking about as well. There is no magic filter that says, "Stop the bad stuff and let the good stuff go through." How do you recognise the bad stuff or the good?

There are many partial solutions. A number of ISPs, including the main one that I use, provide some malware filtering facilities, and that sort of works; it is part of the basic price. This may have come up in Richard's evidence or perhaps he mentioned it earlier, but the next stage is for somebody to provide a response when a user says that they have a problem. In other words, is there a helpline? Helplines are colossally expensive in relation to what people are paying monthly for internet access.

Q20 Stephen Metcalfe: You said that there was no magic filter, although your internet service provider has a form of filter.

Professor Sommer: It looks for basic malware and spam.

Q21 Stephen Metcalfe: Are you saying that it will not find it all?

Professor Sommer: No.

Q22 Stephen Metcalfe: As an aside, some commercial companies are saying that they are going to operate a virus and malware protection system based on Cloud that is away from your machine. Is that going to work?

Dr Clayton: No; it is not going to work for the simple reason that malware has changed. We are no longer in the ’80s, when there were six different forms of malware a month, and everyone spotted them 100%. There are literally millions of bits of new malware a month because nobody has the time to pull them apart, and they have been made deliberately so that every single instance is different. They are, therefore, very challenging to filter. The detection rate on brand new malware is somewhere in the region of 30% to 40%, if that. That is easily explained because the bad guys test the malware and only issue it once it is no longer being detected. Even after a month or so, the detection rate rises to about only 70%. Basically, malware detection does not work terribly well. Mandating ISPs to provide this as some way of fixing the problem is not going to do that, but it will cost a lot of money and give people a false sense of security.

Dr Westmacott: If I may, I shall follow on from that and speak about the sources of malware, where malware comes from, and the reason why there are so many different types. There has been a proliferation of automated malware generation tools; these are toolkits which can be purchased online, which can generate—

Chair: We have been given a very good demonstration by a couple of companies.

Q23 Stephen Metcalfe: Are those who have malware protection installed on their equipment any better off than those who do not?

Dr Clayton: They are a little bit better off because they may be lucky and the malware is actually detected.

Q24 Stephen Metcalfe: But it is not a silver bullet.

Dr Clayton: It is not a silver bullet, no.

Professor Sommer: Most security is about reducing the risk; it is not eliminating it.

Q25 Graham Stringer: You started to answer this in response to my earlier question. Are the problems surrounding smart phones substantially different from the problems with PCs and laptops?

Professor Sommer: They are different in scale, for two reasons. First, because of the way that cell phones are sold, you are induced to buy a new contract on the basis of having a brand new phone. The development cycle for new phones is much quicker than it is for producing operating systems, and as they become more complex there is a greater opportunity for mistakes in design. That is one aspect. The other aspect is that, if you want to correct a conventional operating system fault, it is relatively easy; you are sent a bit of code and you may have to reboot. As you are doing it, you are cursing the waste of time while that happens. However, the operating system and the applications of the smart phone are in firmware, and the business of changing that is altogether much more dramatic and frightening, because there does not appear to be any easy way back. You have to connect your smart phone to a computer, and there is a long period when nothing very much seems to be happening. If the power goes down in the middle of it, you could end up with what is technically known as a brick. Physically, on the outside, there is a smart phone but it has no functionality. That is a great problem.

Dr Clayton: I am much more sanguine about what is going on in the telco market, for the simple reason that the telcos have, over history, taken the view that all the traffic on the network is theirs and the devices are theirs. As a result, when malware is distributed for smart phones, the telcos take it off again. We would not tolerate that with our computers in our front rooms, with the ISP suddenly coming along and saying, “We’re terribly sorry; we don’t like that piece of software that you’re running. We’re going to take it off.” We would not tolerate the sort of monitoring that the telcos do. The telcos do it because they are trying to prevent toll fraud. People defraud them by making free calls and so on. The telcos come from a tradition of monitoring their networks and so forth that is completely different from the internet. It is a much more closed system, and they are much more in a position to control what is going on. As smart phones start using the internet more, not across telcos but starting to use wi-fi devices and so forth, that may change. But the philosophy and the general attitude taken by the telcos is so different that I do not see malware on smart phones being a huge problem for the next few years.

Q26 Stephen Metcalfe: The Government have a duty to protect their citizens from crime. Much of what is being done here is crime; crime has criminal intent. Should the police be treating it with the same severity as any other crime, bearing in mind that the consequences are often equal to other crimes?

Dr Clayton: I would say yes, but you have to accept that, if you are burgled, the police will not pay a great deal of attention unless there is blood on the floor. We have to see cyber-crime in the same way. It would be a shame if you were being defrauded, but we are looking for the equivalent of blood on the floor.

Dr Westmacott: We need to gather far more information on the prevalence of criminal activity and individual occurrences, and we need to provide the public with the ability easily to report information on malware and to say when specific crimes have occurred. Without that information, it will be difficult to move forward with law enforcement.

Professor Sommer: You must understand that the funding for tackling cyber-crime comes from the same pool of money as everything else and there are many competing demands—bobbies on the beat, dealing with antisocial behaviour and so on. Specialist police officers have been putting in a great deal of effort to develop a strategy. You will probably hear about that later; it is in the Home Office document. I think they have got the balance about right.

All of us here are intensely aware of cyber-crime. I act as an expert witness, so I naturally think that a great deal more time and money should be spent on it. On the whole, the strategy being developed is for all police officers to have some awareness, for all detectives to manage and understand digital evidence to a certain level; and we need an elite body that is able to tackle the more complex issues. That strategy is broadly correct. My big concern is that we have a proliferation of overlapping agencies, but I covered that to a certain extent in my written evidence. I hope that you will be pressing the police and the Home Office when they give evidence on why so many different agencies are needed. You will note that they all claim to be covering the big websites where card information is held. Is it right that they should all be doing that, because they appear to be stepping on each other's toes, in my view?

Chair: Gentlemen, it has been a most informative session, and I am very grateful to you for coming in. You have been incredibly helpful to our inquiry.

Monday 14 November 2011

Members present:

Andrew Miller (Chair)

Gavin Barwell
Stephen Mosley
Pamela Nash
Graham Stringer
Roger Williams

Examination of Witnesses

Witnesses: **Gordon Morrison**, Director of Defence and Security, Intellect, **Janet Williams**, Deputy Assistant Commissioner, Metropolitan Police, **Charlie McMurdie**, Detective Superintendent, Head of Police Central e-crime Unit, and **Lesley Cowley**, Chief Executive, Nominet, gave evidence.

Q27 Chair: I welcome you all to this session. It is a bit unusual for me to know all four witnesses before us. Of course, that doesn't mean it will be a totally friendly session, but I'm sure it will be very informative. Obviously, Parliament has taken a close interest in this area in the recent past—there have been a number of very well attended events in the House recently—but clearly, as you all know, we need to be as far on top of the problems as we can. May I ask you to introduce yourselves for the record?

Gordon Morrison: I am Gordon Morrison, Director of Defence and Security for Intellect, which is the trade body for ICT in the UK.

Janet Williams: Hello. I am Janet Williams, Deputy Assistant Commissioner in the Metropolitan Police. I am the ACPO lead for cyber-crime nationally.

Charlie McMurdie: Good afternoon. I am Charlie McMurdie, Head of the Police Central e-crime Unit.

Lesley Cowley: Good afternoon. I am Lesley Cowley, Chief Executive of Nominet, the .uk domain name registry.

Q28 Chair: You are all very welcome. Between you, you have a very wide-ranging set of responsibilities for creating and maintaining the internet, regulating the industry and policing the users. What is your biggest fear for the internet with regard to malware and cyber-crime? Who's going to start?

Charlie McMurdie: I'll dive in. For me, it is loss of public confidence in utilising the internet. That's probably one of our biggest fears, rather than an attack per se. It is that public confidence factor.

Lesley Cowley: For me, it is about better protecting people and businesses and also people and businesses being able better to protect themselves.

Gordon Morrison: The internet clearly provides social benefit and growth opportunities to UK technology and industry, so for us, the biggest fear is that things like malware will create a drag on those two advantages of the system.

Janet Williams: I suppose for me the fear is of this mutating into something even more difficult for us to police. At the moment, we are seeing the attacks quite squarely in the crime area. I suppose my greatest fear is that this could migrate into cyber-terrorism.

Q29 Chair: It would be possible, of course, to create a safe area—a safe haven—inside cyber-space that guaranteed a greater degree of security but would inevitably have restrictions within it. Is that a good idea? Should we think about things such as that?

Gordon Morrison: Yes. There are potential technology solutions to provide a safe-for-anyone internet, but that has to be balanced with the freedom that needs to be provided—the openness of the internet and the neutrality of it. There is a balance.

Lesley Cowley: I don't feel there is a silver bullet. In particular, there isn't necessarily a sole technical silver bullet. For me, this is particularly about education and knowledge so that people can use the net safely, and about finding better ways to increase that knowledge without scaring people completely. Some recent research from the Oxford Internet Institute showed that some people who hadn't used the internet were quite frightened of doing so. I think that is counter-productive.

Charlie McMurdie: We currently have different secure networks within law enforcement or for intelligence sharing or different vested groups. I don't think that is the answer on internet safety or security. There will never be one completely secure environment. There will always be that vulnerability, and that is more often than not the human vulnerability that has to access that data silo.

Q30 Chair: Is that partly because, just as in every other part of the world where people are exchanging information and trade is going on, there are bound to be criminals on the edge of it who have an interest in exploiting it?

Charlie McMurdie: You always have to have a doorway in and a doorway out, so that is the vulnerability that exists. We have seen recent attacks on very high profile infrastructures where you would expect the highest level of security but which have been found vulnerable. Everybody now relies on the internet for their daily working lives, social lives, commerce and so on, so it is about mainstreaming the standards of security and the public knowledge and responsibility to use it safely and securely, rather than creating strongholds in bespoke locations.

Q31 Gavin Barwell: When something goes wrong and a computer user is affected by malware, where should they go?

Charlie McMurdie: A piece of work is ongoing at the moment in the National Fraud Reporting Centre to increase its capability to take cyber-crime reports. That is being developed and is due to go live, I believe, later this year. We are doing some work with the centre to make sure that infrastructure is stood up and the appropriate data is captured. Currently, the advice is to report it to your police officers. We all know, though, that if members of the public have had their identity compromised and they have lost money—they have become a victim financially—their port of call is to report that to the banks, where they are reimbursed for their loss. That doesn't mean to say that we lose the intelligence around that compromise taking place, because we have a process where the data captured by the banks is reported into the financial intelligence system and then collected as, "This is the number of people who have been defrauded". We are increasing law enforcement capability. One of the programmes under the DAC is to actually roll out mainstream training and awareness for all our 140,000-odd police officers, so they will be better enabled to take crime reports from victims of crime, but also to provide that investigative capability to those victims.

The big point of reporting or contact, as far I am concerned, is within our virtual taskforces where we have groups of people, whether it is the financial institutions or security bodies, who come together as a collective with a common threat or problem, and then they can brigade their intelligence to that report and report that to law enforcement to do something about it.

Lesley Cowley: I think there is a role for industry here as well, though, in terms of educating businesses and consumers, but also signposting where to go if you have a problem. Certainly Nominet, for our part, have a service we call "Know the Net", which is about signposting and helping to educate people and directing them to the right place, whether that is with Get Safe Online or other actors in this space. So there is certainly something very much around industry working in partnership with law enforcement and other agencies.

Gordon Morrison: There is a lot of best practice out there worldwide and in the UK, so what is really needed is a laser-like central point of reference on where to go for them. Get Safe Online may be the right place for it, to tell people how to protect themselves, what to do if there is a problem, and also to refer people to things like the malicious software removal tool that certain companies provide. So there is lots of technical stuff out there that can remove the code, but also lots of good practice. The general public, the SMEs and the large companies need to know where to go for that. The problem is that it is pretty much spread around.

Janet Williams: I don't think we are as good as we need to be in policing, in terms of every single police officer in this country being as equipped to give a member of the public a piece of advice around cyber-security as they are, for example, for their windows and their doors—their general house issues. The other bit for me is that we have security co-ordinators who talk to smaller businesses and medium-sized businesses about their security, generally. They actually go to those premises and give them some good advice, and they are trained to that effect. We need to enhance their roles perhaps and give them the skills, capability and capacity to actually go to organisations, sit with them and help them do this thinking. Once they have some confidence that someone has sat with them and actually helps them do it for the first time, then they will feel equipped to go to Get Safe Online and, in the future, take advice via the internet. But in the first instance, I think some businesses just don't have that confidence and need someone to hold them by the hand and take them there.

In policing terms, I would want to be in a position where every police officer has a basic level of training, and it gets better and better and better depending on their role: if they are a detective they have one set of skills; if they are in one of our regional hubs, they have another set of skills; and when they are in the central PCeU doing the high-level cyber-crime, of course they have the top-level skills. That should be complemented by a series of security co-ordinators who could go and hold small businesses by the hand in the first instance, and give them some good guidance.

Q32 Gavin Barwell: Am I being unfair to say that you have all given very informative and useful answers, but with slightly different emphases? Should I read into that that there is not yet complete clarity about the first point of contact I should go to if something gets on to my computer? Am I being fair in deducing that from your answers?

Janet Williams: *Indicated assent.*

Gordon Morrison: *Indicated assent.*

Charlie McMurdie: *Indicated assent.*

Q33 Gavin Barwell: You mentioned Get Safe Online. There is a lot of information there, both on use and on how to avoid harm. Do you think the site is well-integrated enough with the places you would then need to go to, as far as services and security are concerned?

Gordon Morrison: Yes, and what I was talking about does refer you to best practice and technical people to talk to. As a technical trade body, we would say that it does not necessarily cover the SME angle and maybe the corporation; it is very much focused on the general public and there may be some more work to do on that. One view in our country is that those running SMEs are the people who need helping to secure themselves. That is one piece of advice I would give.

Lesley Cowley: This goes to my point earlier about this being not a single responsibility but a shared responsibility. It is quite unusual, I suspect, for an end user to know exactly what the problem is, but they know they have a problem. Whether people contact their internet service provider, look online to find solutions, or go via trading standards or their local business association, it is important that they have some knowledge and know where to send people for help. There may be quite a range of actors in that space—certainly from my point of view one key thing is the education of businesses and end users, so that they can keep themselves safe too.

Q34 Pamela Nash: A recent report from the McKinsey Global Institute showed that e-commerce in the UK makes up 6% of the UK's GDP, and 21% of growth in GDP, and the Minister Francis Maude recently said that the UK is currently Europe's leading e-retail economy. Gordon and Lesley, do you feel there are indications that the UK will continue to be such a sought-after place in the world for e-commerce? Are there any concerns that would inhibit that growth?.

Gordon Morrison: Yes; we are definitely targets, as are the US and the western world, mainly because of our e-business. I do not see that changing—perhaps we should ask the police officers. I think we must recognise that we will—I hope we do—use ICT to grow and maybe get ourselves out of the deficit. I don't see that changing.

Janet Williams: I think prosecution is really important in this, and I think that cyber-criminals should not feel safe. Although there is a great emphasis on prevention and on patching systems—all of which is very important—I think that prosecution is equally important. The police e-crime unit under Charlie has done some really good work. The way we work with industry now is quite unique in that previously, industry would hand us an intelligence package and expect the police to get on with it. Now, we work hand in glove with industry, and we are using its people and kit alongside our people and our kit, which enables us to cross jurisdictions. We know that cyber-criminals don't like this and that they are getting quite nervous about that capability. I think that is a good thing; we need more of that because it is obviously working. We know it is working because in the first six months of this year, for every £1 invested we have recouped £35 of harm. That means that we have saved the UK economy £140 million in the first six months alone. The proof is in the pudding. One, cyber-criminals are getting worried about us, and two, we are mitigating that level of harm.

The fact that we are now bringing all our capabilities together will be of benefit. The Cabinet Office initiative of getting the security services working with policing and industry, with everybody sharing information and helping each other to understand the problem and move forward, has got to be of benefit. That is something that this country has a really good history of and certainly in counter-terrorism—where I currently sit—we are known for our expertise in that sort of crime. Part of that is because we are good at sharing information and intelligence with security services and policing. We should build on the strong foundation in that arena, and the Cabinet Office initiative will help us do that.

Q35 Chair: May I just interrupt you there? In the earlier part of your answer, you seemed to indicate something that is, I think, a subtle but important change in position from the police, which is that crimes ought to be prosecuted in this area. There was a period when the attitude was either that we haven't got the resources—I understand that—or that it is a victim-less crime and whoever it is will pick up the tab.

Janet Williams: It has never been a victim-less crime. Sometimes it is difficult to determine exactly who the victims are, but that is usually because of the quantity of victims, so it is hard to put a name to it. It is damaging our economy and our citizens and we should be very clear about that.

Yes, policing did struggle because we did not have the resources, the capacity or the capability to deal with this level of criminality or the way in which it was developing. I think we are getting there now. There are 104 people in the police e-crime unit. We started from a very small number, so we have increased massively. The next step in this financial year is that we will be building three hubs: one in the north-west, one in Yorkshire and Humber and one in the east midlands. They will link into the police e-crime unit and have a symbiotic relationship with that unit as well as being able to be leaders in the region in which they are situated. They will be able to take on this sort of criminality in their own right and, like the police e-crime unit, they can advise other serious crime units. If units are dealing with people trafficking or with drugs, the hubs will enable them to understand the cyber aspects as well as dealing with the pure cyber criminals in their own right.

Q36 Stephen Mosley: I was pleased to hear what you have just said. You were talking about banking earlier, and there is a perception that if money goes from your bank account, you speak to your bank and you might get your money back, but it doesn't seem to go any further. Have you any statistics on how many prosecutions and successful prosecutions there have been over the past three or four years?

Charlie McMurdie: Certainly. We have arrested about 123—numbers do not really mean an awful lot, and that is an approach that we have changed. There have been 124 arrests, 32 so far found guilty. The numbers are not the key point that we are looking at. We could arrest 200 people tomorrow, but they may be low-level users of compromised data. Where our taskforce focuses its activity is working more often than not with the financial sector—all the banks coming together—where it would potentially have tens of thousands of victims. The banks work with us to identify the higher echelon of criminality that is responsible for the harvesting or selling of those data, or the compromised process of disseminating the malware to harvest thousands of computers to use them for attack purposes. It is about taking out the root cause—the two, three, four or half a dozen instances of top-end criminality before they get to the lower foot soldiers.

As to numbers of individual cases currently running through the courts or being prosecuted, we had another case concluded last week. Eastern Europeans had compromised tens of thousands of identities and run them through the UK infrastructure. They were facilitating global criminality, so in that instance they were writing the code, constructing the code and then using the code for financial gain. That could quite easily have been turned for attack purposes. To take out that higher end criminality is quite a significant result for us.

Q37 Pamela Nash: Can I ask a short question? With all the work that you are doing and that you have just detailed, do you feel that the message that it has been successful is getting through to industry, and have you seen any evidence of a positive response?

Charlie McMurdie: Most definitely yes. We have had that intelligence; it is getting through to the criminals, because when we do take out some of these higher-end criminal organisations we can see the intelligence behind that, and see that level of criminality move elsewhere; or the criminals will decide not to attack that sector because they have been detected. They will move somewhere else.

Certainly there is feedback that we have had from industry, which is encouraging more reports and more intelligence with us—that is how we have developed—and industry is seeing positive results as a result of us working with it and arresting and prosecuting these criminals. That is where we get the main source of our intelligence and learning as well, when we sit face to face.

You have heard the unit is now 104-strong, but I think certainly the Police Central e-crime Unit is probably one of the best cyber-capabilities now, worldwide, because of its success. But it is not just because of the 104 staff I have; it is because of the reputation and the way we work with our partners—our industry partners, our other law-enforcement partners, both here in the UK and abroad. We are a hub of 104, but we can call upon massive resources from elsewhere.

Janet Williams: There is one thing I am a little bit worried about, that it would be helpful to have some support on. We are just about to look at the strategic policing requirement nationally, and for me it is really important that cyber is identified within that requirement, because if it is not I think chief constables and crime commissioners may not feel that they have to put the resources in the infrastructure in place to deal with this locally. Part of our strategy absolutely relies upon local police officers being able to deal with the low-level stuff, as I described before; the regions taking on some of the regional capability and then the PCeU dealing with the high-level stuff. If that is not in the strategic policing requirement I am afraid it might not happen, but that is one thing that I would really appeal to the Committee to help with.

Pamela Nash: Thanks for putting that in.

Lesley Cowley: Your original question was not really about policing, necessarily. It was about the internet as the engine-room for growth. I think one of the reasons why the UK has been so successful is that we have very much viewed the internet as an enabler. We have taken a light-touch approach to regulation, and there has been a lot of industry-led information-sharing, knowledge-sharing and self-regulation, in effect. I do quite a lot of work internationally and the UK is well known for taking and supporting a multi-stakeholder approach, which I think has been absolutely key to some of the UK's success in the internet economy.

Q38 Pamela Nash: A lot of the submissions that we have had in this inquiry have referred to that, but there also seems to be a bit of a thirst for some leadership. Do you think there is a role for Government to take the lead?

Lesley Cowley: I think there is, potentially. I think there is a role for Government to take the lead in partnership with industry and the other actors. Going back to your earlier question, certainly in discussions internally we have talked about the need for some sort of internet CERT, a place to share information about opportunities, threats and innovation. That would be helpful. Government can also take a lead by adopting some of the security standards at an early stage and showing leadership, and facilitating that approach going forward.

Gordon Morrison: Perhaps I can come in on that and say there is recognition that certainly industry is focused on growth and risks; there is a need to do some work in the UK, which perhaps Government can help us with, and there is some work that Intellect is doing about really focusing people on the risk of cyber, and perhaps the opportunity of cyber. That way people can invest and protect themselves.

To comment on what the police service said—I commend the work that has been done in the police in the virtual taskforce and financial services—a lot of members' views in industry are that penalties for producing malware and doing cyber-crimes are perhaps not as hard and as long as they should be. It is not a criticism of the police service; more of the penalties.

I think the other thing—I just recommend this as a remark, really, from north America—is that certainly in north America the view is we should help people take civil law suits seriously, and have civil prosecutions against cyber-criminals.

Q39 Pamela Nash: I have a couple of specific questions about the .uk domain. Is there scope to make it a more tightly regulated place when it comes to malware? Could that alter the conduct of e-commerce in the UK?

Lesley Cowley: If you are talking about Nominet and .uk, we already do a great deal to make .uk a great place to do business. We have certainly done some recent work on DNSSEC—the enabling and security extensions—which will go some way towards what you describe. We do quite a lot of work in co-operation with law enforcement and others, both nationally and internationally. We are also doing some work on data quality to help make .uk a less attractive place for criminals and others who might put out incorrect information, shall we say. We are certainly aware from independent research that .uk is a very trusted place to do business, and people actively prefer a .uk website over a .com website. It is important we retain that reputation and that trust.

Q40 Pamela Nash: There is continual work going on to ensure that is the case?

Lesley Cowley: Absolutely. All the time.

Q41 Pamela Nash: Does everyone agree with that?

Charlie McMurdie: We work closely with Nominet. We have limited resources, but Nominet acts as a point of contact for industry to reach out to when it identifies rogue or fake websites, or websites that are being used to disseminate malware, for example. We will look at investigating those sites and producing agreed standards of criminality, and we have a process in place for referring sites to have them suspended where criminality is taking place on them. But as you have heard, it is an ongoing, developing, improving process, with better co-ordination around that.

Gordon Morrison: The only comment I would make is that we have a very good .uk domain, which is very professionally run, and we have a police service that is very focused on security. Our focus should be on education from schools all the way up to shareholders. This is not a technical issue; it is about people understanding not to click on certain things or not to read spam—the hygiene around using your computer, the green cross code for your computer.

Pamela Nash: Thank you.

Q42 Chair: Before we move on, Miss McMurdie, given your relationship with Nominet in the UK and your experience of dealing with police forces around the world, are there lessons we could learn from other police regarding domain name registers that would improve things here, or are we the leader in the world?

Charlie McMurdie: I think we probably lead the way, sir, with the process that we have in place. Obviously, the sites we are asking to have suspended are in a lot of countries, and a number of the operations we have conducted involve sites hosted all over the world. In a recent operation, we took down sites in 186 different countries, and we have suspended thousands and thousands of sites. More often than not, if they are in more remote countries, we will work with the top-level domain name registrars; we will work with industry, rather than go through the law enforcement group, which, quite often, is found wanting in some other countries. Particular problems happen to be in America, surprisingly; a lot of the infrastructure is hosted over there, and it tends to be a very slow and cumbersome process to get any form of response or action regarding sites in the States.

Stephen Mosley: I think most of my questions have been answered, Chairman, so it might be worth while moving on. Perhaps a bit later I can chip in on a question.

Q43 Graham Stringer: E-crime is a new crime. I guess when you were doing your training, it was not high on the agenda. When it is difficult to detect, capture and prosecute the criminals, how do you prioritise e-crime against other police work?

Janet Williams: That is where the strategic policing requirement comes in. ACPO has tried to push the cyber-portfolio up the agenda. To a certain extent, it has achieved that, hence the agreement about the three hubs and the comprehensive agreement on police officer training right across the country. We have never really had a comprehensive understanding of how significant this crime is, and we have never had a comparison with other crimes in the way that the strategic policing requirement will give. That is why I am so keen on influencing it.

Q44 Graham Stringer: If I understand that answer properly, I guess that means you have real difficulties in recording crime.

Janet Williams: Yes.

Q45 Graham Stringer: And knowing whether you are detecting a greater percentage of it or improving. Can you talk about how you record a crime, how you would test and communicate improvements in your technique, and the size of the problem you are dealing with?

Janet Williams: We have already covered some of this, but for me it is about no single point of reporting; everybody knows where to go in the case of a burglary or a rape. I do not think there is the same level of understanding. Also, some organisations do not choose to report, because it might be sensitive to the share price in that organisation. They may feel that they really do not want this to come into the public domain, so we lose a great deal of understanding and intelligence as a result. Currently, there is no obligation on business to report. What we get is fractured, because there is no single agreed point of reporting. Even what we do get is not a full picture, because some people just choose not to report.

Q46 Graham Stringer: You are answering lots of questions before being asked, which is an advantage.

Chair: It is the intelligence unit.

Graham Stringer: Are the operational responsibilities in different parts of different police forces clear?

Janet Williams: With the exception of the Metropolitan police and the police e-crime unit run by Charlie at the moment, in terms of this high-end cyber-crime investigative capability, it only exists in that one place. We try to fulfil that national function, which is what we are supported to do financially. That is what is in our strategy. In terms of capability elsewhere across the police service, it varies, depending on where you are. There are some pockets of really good capability in Scotland and the north-west. I am sure Charlie knows other areas too. It is not comprehensive and it is not co-ordinated in the way that we want it to be, but it is part of our strategic direction. That is what we have some of the money for. We are on a time line to deliver it by 2014. We are working to that time line, and in fact are ahead of it, but by no means is it comprehensive coverage now.

Q47 Graham Stringer: What are the advantages of the new unit in the National Crime Agency over what you have at the Met and in SOCA?

Janet Williams: What is really important to me when we migrate to the National Crime Agency is that everything that the police e-crime unit has succeeded in doing—building relationships with industry, developing capability and capacity, improving our intelligence capability, but most importantly, going after criminals, being good at that, capable of doing that and very operationally focused—needs to be retained. The benefits could be that if you co-join with SOCA and other agencies—that is the key—it should be greater than the component parts. What is important is that the capability should support the other strands of the National Crime Agency, building much better, faster, cross-jurisdictional reach and intelligence-sharing. Much better relationships with the security agencies should enable us to step change. For me, there is no point in the police e-crime unit migrating to the NCA if the NCA is not better than its component parts. That, absolutely, must be our ambition. We must protect what we already have and enhance it.

Q48 Graham Stringer: You have mentioned a number of times the benefits of working with the security services. How do you work with Interpol and Europol? Or do you work with them?
Janet Williams: We do not do much with Interpol to my knowledge—Charlie might know better than me—but we have done quite a bit of work with Europol. We have some taskforce work, but Charlie knows more about that, I think.
Charlie McMurdie: Europol is slightly more tactical than Interpol in our engagement. Certainly we attend the Interpol working groups as one of the UK Interpol representatives. Interpol is looking at more strategic, international engagement, learning and process-type work. It is moving towards being more around training standards, whereas with Europol we have a number of groups looking at common legislative problems and issues, common training standards, building training modules and tactical data-sharing. We can task Europol some of their analyst capability, or task out packages of work through Europol. For example, some of our joint investigation treaties are established through the Europol route. So it is far more tactical, currently, through Europol, rather than slower-time, more strategic work ongoing with Interpol.
That said, we have just conducted a recent operation—website suspension work, with rogue medical websites—with 80-odd countries, which was co-ordinated by the Interpol control centre. It provided capability for us and put all the various points of contact in place. But far more work is with Europol, currently. Interpol is just relocating as well, so it has been through quite a move; it is looking at bigger growth, to put in more capability.

Q49 Graham Stringer: My last question. E-crime must be the easiest crime to do internationally. Are there any areas where relations with other countries or other agencies could be improved, on an international basis?
Janet Williams: Quite a lot of different countries. We have a considerable resource in SOCA, in that it has developed really good international relationships. Most definitely the police e-crime unit piggybacks on those relationships, which is quite right. As we draw closer to the NCA, I think that will become more and more apparent. We have tried not to create our own independent relationships and duplicate effort. We have tended to piggyback on the SOCA relationships and to develop them in a more proactive and operational sense.

Q50 Stephen Mosley: It is the international dimension I was interested in. Do you have any indication of how much the crime committed against people in the UK actually originates outside the UK?
Charlie McMurdie: Every investigation that we conduct has suspects based internationally or money flow that will travel internationally, or the attack will be facilitated through international sites, servers or systems. So every case that we deal with requires international co-operation, parallel investigations, data from abroad, and the way that we have to work is on a police-to-police basis; cyber is too big, too fast, to run through our existing law-enforcement MLAT process. An attack is happening this evening at 4 o'clock, and we need to have 10 or 12 different countries on the line responding within the hour to do something about it.

Q51 Chair: That presumably will include everything, from the minor scams that are targeted at large volumes of people all the way through to the spectrum of criminality that occurs on the net?
Charlie McMurdie: Primarily, the fastest time response that we need to put in place is when an attack is live—is happening—and they are taking out some particular infrastructure, so an online service or function—

Q52 Chair: Sorry, but you have misunderstood my question. Your answer to Stephen's first point was that everything has an international dimension. I am just asking you to confirm that the whole spectrum of criminality has an international dimension.
Charlie McMurdie: More often than not, yes. Even if we forget cyber-crime and the high-end attack-type stuff and look at something simple, such as somebody sending some cyber, internet bullying-type message, or stalking somebody online, that is probably hosted on some Hotmail or Yahoo! account, and the IT and the data that we require will be hosted in a different country.

Q53 Chair: There are two officers with considerable experience here. Does that require a different approach to law enforcement and crime detection from that for crimes that are from a static location?
Janet Williams: Yes, I absolutely think it does. First, the legislation is not fit for purpose and we need to bring it up to date to deal with this, but we also need a much more dynamic response. If you think about prevention in traditional terms, police officers would normally look at a series of crimes, take the learning out of that, think about it and issue good practice, and people would then adopt those as prevention measures. We haven't got time in this arena to do that. We are having to act dynamically to patch systems, to warn people about how they might protect themselves in order to prevent the spread of a virus infection, for example. The speed is different, the calibre of officer you need who has the technical skills to do that is very different, and the legislation that backs you up has to be very different, so this whole thing needs to be looked at.
We are very fortunate that we have managed to identify some very experienced detectives to work for us in the police e-crime unit, but it takes about seven years to get someone up to the level that we require

to do the sort of work that we are asking them to do. You don't need that many of those people—you can have less skilled people supporting them—but you absolutely do need a core. There aren't that many people in the country able to do this, and we are constantly seeing leakage into industry, which is, frankly, poaching, because, of course, everybody wants these people. For me, the way that we think about this has to be very different.

Q54 Chair: May I test you a little further on this legislation that has to be different? I presume from that that you need legislation that creates a framework within which you can work while giving you a great deal of scope to move fast within it.

Janet Williams: Absolutely, within the law, so that we can protect UK interests and UK people whose data is often housed outside this jurisdiction. We need to be able to protect it.

Charlie McMurdie: A key part of our remit of arresting and prosecuting people is to make the most out of the learning, the intelligence—both the strategic and the tactical learning that comes out of our operations. That is what we feed into. We have established a Home Office group to look at some of that learning, some of the gaps in our capability, and opportunities around legislation.

Q55 Stephen Mosley: From what you have said, it sounds as though you have the capacity to do the investigation side, but you also talk about crime prevention, which the police would normally do, and it sounds as though, because of the expertise you need, you probably aren't able to do it yourself. Who do you think should take the lead on educating people in schools, and on crime prevention? Lesley talked about a multi-stakeholder approach. Is that multi-stakeholder approach suitable, or do you think someone should be given the task and told that their job is to lead crime prevention and to bring together the vendors, the industry, Nominet and yourselves?

Charlie McMurdie: I think BIS already has programmes of work ongoing, and linking through with Get Safe Online, but I think there is a real gap and an opportunity where we need to have physical representatives that people who have been victimised or need advice can turn to, whether they sit under law enforcement as our SECCOs—crime prevention officer—or whether they sit as sub-people working to get safe on line. But those individuals don't currently exist, and I think there is a real opportunity to work with the industry to put someone of that nature in place. People don't look for advice on what they should have done or how they should have dealt with things until they have been a victim, when it is too late. It should almost be at the point of manufacture, point of sale, or point of education. The use of the internet is an integral part of everything we do. It should be integrated into our schooling processes. It is too little, too late.

Janet Williams: Someone said to me that we all understand that we won't walk down a dark alley in preference to a lit alley. That is instinctive, and we almost need to get to that point with this, so that people understand what the danger signs are, and at the moment most people don't.

Q56 Chair: I suggested at the Get Safe Online briefing that was held here last week—it produced a very good online leaflet—that we want perhaps to work with retailers, particularly in the high street, and persuade them to carry that and make sure there is always an up-to-date version of it that goes out with every piece of kit that is sold. Would you agree?

Charlie McMurdie: That is an excellent idea, and I think there is work ongoing with some of the staff of particular electrical stores—I won't name the shops—to increase their training and capability to advise people on the security aspect when they are buying something, and to give them that type of leaflet.

Gordon Morrison: Yes.

Charlie McMurdie: Excellent idea.

Gordon Morrison: I would argue that it is people who control the problem, from school leaver, schoolchild or whatever to shareholder, and the industry and the police service can help that. The real issue about social change in the UK is that it is at national level. It is even like TV adverts or the old public information service of years ago. It is about making people realise how big a problem this is. I don't think we have got that. I think we have the components, but people don't really understand quite what the threat is.

Q57 Chair: I think some of it is there. I rather like the HSBC advert with the little girl opening a magic money box, for example. It is a very clever message. We want to see that penetrate right through society. I think that is a problem we can all agree on. The Minister is sitting behind you absorbing all these ideas, and feeding them into the autumn financial statement. I thank you all for attending.

Examination of Witness

Witness: **James Brokenshire MP**, Parliamentary Under-Secretary of State for Crime and Security, gave evidence.

Q58 Chair: Welcome, Minister. I was delighted to see you listening in to the previous session, because we had what I think you will agree were four extremely well informed witnesses.

James Brokenshire: You had several experts in their field and it was very interesting for me to sit back and listen to their contributions as well, so thank you.

Q59 Chair: We are obviously waiting for the announcement of the cyber-crime strategy. Could you explain to us what you consider to be the key issues in tackling malware and cyber-crime?

James Brokenshire: There are three key themes that we are looking at in the cyber-crime and cyber-security strategy, which we will issue soon. The first is reducing online vulnerability, through a programme to improve security and the steps that people take in terms of the purchasing and design of software and systems, as well as public awareness, education and some of the themes that you touched on right at the end of the preceding session.

The second theme is restricting online criminality, by having the right laws and the law enforcement response in place to ensure that those who seek to commit cyber-crime can be prosecuted.

The third theme is what I might characterise as the co-operation strand. That is co-operation between citizen, Government and business, as well as co-operation between Governments, recognising very clearly the international aspect to this crime, which is probably above all other crimes in the way that everything connects up.

It is those three strands that I would perhaps focus on in setting the overall framework to the approach, given that I do not think that there is one single answer to this issue. There has to be an approach that takes a number of different steps and covers that broad range for it to be effective.

Q60 Chair: The Government announced a substantial sum of money for tackling cyber-crime—£650 million. Of that, £63 million will be

"enabling the UK to transform our response to cyber crime".

In your previous answer, you recognised that this is a problem facing business, Governments and the whole of society, including individuals. How much of that money will be apparent to individual computer-users?

James Brokenshire: As you heard in the previous session, investment is going into law enforcement capability and capacity. Therefore, I think that the response that the public receive around cyber-crime will be enhanced by the investment that takes place. We are moving to a new policing environment and the establishment of the National Crime Agency, to which I am sure we will turn in further questions. Again, I believe that that will enhance that capability further by drawing various strands of law enforcement operations together, so there will be that sense of seeing a step change.

Clearly, we are also looking at the educational side of this issue. The Office of Cyber Security and Information Assurance in the Cabinet Office, are working closely with BIS and other Departments, including the Department for Education, to look at how we can better impart some of those educational issues. We will also focus on skills, to ensure that we have people who are appropriately skilled to provide that response.

I think that there will be visibility to this approach and I think that we are already starting to see that, but clearly one of the challenges that we face is getting the positive information out there in terms that the public understand. I think that in some ways we wrap a lot of this information up in technology-speak, which sometimes makes it a little bit impenetrable for the public and others to have a sense that it is directly relevant to them. The communications strategy must have that idea at its heart.

Q61 Chair: We had a very similar discussion with Anne Milton recently, in the context of how the public understand and respond to advice on alcohol. Do you see this as a similar thing, in terms of the way that public health messages need to be transmitted—not in "doctor-speak" but in "human-speak"?

James Brokenshire: It needs to be imparted in that way. Sometimes, when I have attended some of the conferences, debates and discussions on the issue, it can at times sound as if you are talking through a complicated plot from a science fiction novel, whereas in fact, what we are talking about is real-life crime and real-life impact. It is actually the language used in some of this. If we simplify it to fraud or some traditional crimes that are committed using technology, breaking it down in this way, we can make apparent to business the reputational risk that they may run if they don't get some of these issues right. That context and relevance is very key in ensuring that that transfers from something that may be viewed as perhaps for the specialists and technicians to something that has a broad and wide impact and application to all of us.

Q62 Chair: You heard my last question to the previous panel about the need for the work of Get Safe Online to reach the customer at the point where they buy their goods. Would the Government consider that to be a useful way of spending some of this incredibly valuable money? You have a substantial sum of money at your disposal, but it must be spent wisely to be of the maximum effect. Is that the sort of initiative you are considering to improve public awareness?

James Brokenshire: We need to consider how Get Safe Online could be more responsive to information or alerts issued by law enforcement agencies or via the new mechanism to enable people to report financially motivated cyber-crime, Action Fraud, which will come online later this year.

Q63 Chair: My particular point was about the point of sale of hardware, where, particularly on the high street, evidence suggests that a significant proportion of the customer base are not aware of the risk they are facing when they first switch on their smart phone or laptop.

James Brokenshire: I am keen to discuss that with business, in terms of what is likely to be efficient and effective. It is also perhaps worth pointing to the example of the UK Council for Child Internet Safety, which I co-chair, and the work that we have been doing with Dixons and Currys/PC World. Those retailers have been putting information on the back of their till receipts about loading up filtering software so that parents become aware of some of the issues for children—the concept of active choice. I am keen to continue discussions with business about what happens when people buy hardware in a shop, but we cannot ignore the fact that, nowadays, most people buy a lot of this stuff online anyway. If the point of sale is migrating towards the online environment, how are we better able to impart those messages online as well as offline in the stores?

Q64 Graham Stringer: Francis Maude gave a speech in which he referred to a survey done by Google, which found that only 5% of internet users thought it was the Government's responsibility to look after the security of their information. Do you think that that means that there is something fundamentally different about e-crime and about the state's responsibility? Do you feel that the state has as much responsibility in looking after the security of information as it does looking after the security of individuals or people's property?
James Brokenshire: I think, Mr Stringer, you make a good point about the differences that reside in this environment. In large part, the infrastructure that makes the internet operate and the way in which information is stored reside in the private rather than the public sector. Now, that does not mean that the Government do not have an important role; I strongly believe that they do, taking the various strands of work that I outlined at the outset in relation to the strategy and approach that the Government will adopt. I think that the Government are instrumental and have a role when we look at the international perspective in bringing together Governments and how the law and law enforcement respond. Indeed, given the way the Government themselves operate, as we move to an online Government world in the provision of services, we will be facilitating and holding a lot of information ourselves, and it is important that we do that right. It is also important, in the design of our systems, that we seek to use that opportunity to perhaps raise standards and ensure that we are influencing things in the right way.

Q65 Graham Stringer: You have suggested a Government portal for providing security information to people. How would that differ from the information that you would get from Get Safe Online?
James Brokenshire: I would certainly look at Get Safe Online as essentially being a platform; you would use it as a mechanism to transfer the information.

Q66 Graham Stringer: So it would be an upgrading of Get Safe Online?
James Brokenshire: That is certainly how I would visualise it. Rather than trying to create something new, I am always of the school that wants to use something that is there and to draw it together more effectively.
Graham Stringer: That is clear.

Q67 Chair: Before you move on, and just to be clear, Get Safe Online is a public-private partnership, so do you envisage the Government taking the lead in putting more money into it and encouraging the private sector to do so as well, or are you just leaving it to the private sector?
James Brokenshire: Get Safe Online has been a strength because it has had that public-private partnership attached to it, recognising and reflecting the challenge that was very much at the heart of Mr Stringer's question about whether this is something that resides in both environments. I would certainly want to see Get Safe Online continuing to have that public-private partnership, but I would also want to look at ways in which we are able to make it more responsive. I would want to look at the information that will be coming through from various different agencies to ensure that Get Safe Online is able to protect the public better so that, if threats and risk emerge, we know how best to impart that information. At the same time, we must recognise that we do not have a monopoly on these things and that there are some other very good sources of information. Recognising that, Get Safe Online can perhaps also act as a signpost to other sources of information.

Q68 Graham Stringer: Here is a conundrum. Get Safe Online has done a survey, and 28% of internet users declined to use security programmes—I do not know whether you are aware of that statistic. Do you think that is perverse wilfulness on the part of nearly a third of internet users, or is it ignorance? Do you have a view about what the solution should be? Should it be just more information—battering these people with more information—or does there need to be a legislative framework to deal with this?
James Brokenshire: I am not in favour of legislation in this particular arena. This is, in large measure, about how we can better educate people and, coming back to my earlier point, about underlining the potential challenges or risks in a way that is understandable, so that people recognise that we all have a responsibility in this arena. Of course, the Government have the responsibility to provide a basis of information for individuals to take up, but there is also a responsibility on business to assist. I sometimes liken this to the fact that we are moving to a system of more online business and online trading, and that facilitates growth and business. If business is taking its customers more down an online trading route, it has a responsibility to support them in that environment and, therefore, to design its systems in a way to aid that process.

Q69 Roger Williams: Good evening, Minister. We have had some written evidence—indeed, we had some oral evidence last week—that suggests the Government have too many organisations with overlapping responsibilities. At the same time, one of the real restrictions on effective police activity is a lack of resources. How would you respond to that suggestion?
James Brokenshire: The Office of Cyber Security and Information Assurance in the Cabinet Office provides the overarching, cross-governmental lead to draw the relevant strands together. I actually think that we have made some very important changes in law enforcement, through the funding that has been provided and as a result of the recognition of the threat that cyber poses. The creation of the new National Crime Agency, with the National Cyber-Crime Unit contained within it, will actually start to draw together some of these strands to ensure that there is a more co-ordinated, more coherent law enforcement response. That will harness the intelligence hub that will be at the heart of the National Crime Agency, establishing the National Cyber-Crime Unit as a centre of excellence so that it is able to work with

individual police forces, as well as being responsive to the complex areas of cyber-crime that are currently being confronted. Those changes will actually join this work up much more effectively. In addition, we will be looking at how to co-ordinate and task work around this arena, working with and through the strategic policing requirements of individual police forces so that they lock together much more effectively. In turn, we are working through that with the security agencies to give coherence to that strategy. So, important work is already in place. We are taking further steps to give even greater coherence to the existing architecture.

Q70 Roger Williams: So you think the central role of the National Crime Agency is that of bringing together of the rather diverse number of organisations to gain some more resource efficiency?
James Brokenshire: The resources have been committed in relation to the scaling-up of activity around cyber. I think the National Crime Agency interlinks the various different strands of work through the commands the National Crime Agency will have, recognising that so much of cyber is organised crime and financially motivated crime. When we talk about cyber-crime, sometimes we can talk about a number of different things. We are talking about high-end, network-based attacks on IT infrastructure—that sophisticated level—but we are also talking about traditional crimes committed in a different way. Now, that new technology may mean that they are committed on a greater scale with greater ease, but ultimately you are talking about things like fraud and theft. Thirdly, it is how technology is being used to facilitate crime, whether that is the online data supermarkets exchanging people’s details, or the use of social networking to be able to facilitate crime. I try to break it down in those three separate pots, in terms of how you might define cyber-crime, give that clarity and then decide what the response should be.

Q71 Roger Williams: How are you going to make a judgment on whether the National Crime Agency has been effective in doing that sort of work?
James Brokenshire: One of the things that has been very clear to me is the need for better information and better data. There have been estimates as to the impact of cyber-crime. The Office of Cyber Security and Information Assurance and Detica produced a report earlier this year suggesting it could be as much as £27 billion, but then what does that mean? How do you then take that forward? That is why we want to establish Action Fraud, which will be a clear reporting mechanism for financially motivated cyber-crimes, so, again, we are getting better reporting and better information, and therefore establishing the responsiveness based on that.
One of the clear pieces of work that we are doing in the creation of the National Crime Agency, on each of the different strands of operation that it will fulfil, is doing precisely what you are saying, Mr Williams: providing that clear granularity to show that it is working, that we are better responsive to these issues, from a base where I think the information is not as good as it should be.

Q72 Pamela Nash: In May, Francis Maude announced that the Government will put in place a digital identity assurance scheme for public services by summer next year. Is this project on schedule and how much will it cost?
James Brokenshire: The project, which, as you say, Francis Maude has been leading on, again brings together Government with other business and other agencies effectively to facilitate better use of services online. In other words, you have your identity online. How better we are able to secure our identities, and therefore to have that trusted identity—if I can describe it like that. To respond to your point specifically, it is intended to provide a solution that can be used for accessing any public service, simplifying your experience when you use services online, as well as ensuring security and privacy. The costs will not be known until the design stage has been completed. That work is underway, so I am sure that we will be able to provide this Committee with more details as that work progresses, but, at this point, because of the design work being in place and that being a key and core part of it, I am unable to provide those figures for the Committee.

Q73 Pamela Nash: Can I take it from that that it is not on schedule?
James Brokenshire: No, it is on schedule. I would not want to give that impression to the Committee. It is about the different phases of work. I know from discussions that I have had with Mr Maude that he is very much driving the process through and wants to see it committed to on time, because of the benefits that we will all get from it, in terms of the way that we interrelate with the cyber-world that the Government will increasingly be evolving into.

Q74 Pamela Nash: I appreciate that, but I believe that the original timetable said that the first prototype would be tested in October, but you are saying that it is still at the design stage at the moment.
James Brokenshire: I would be very happy to write to the Committee to confirm the different levels and stages of work, because it is something that the Cabinet Office has been leading on. I certainly recognise the importance of it. If we are able to ensure the good use, and safe use, of online services through Government, we need to have greater assurances for the use of our identities. I will certainly confirm and double-check for this Committee on the progress that is being made in relation to that particular project.

Q75 Pamela Nash: Thank you, that would be really helpful. We discussed this in last week’s evidence session, when we heard evidence from the academic community. Although it was accepted that this might be a useful project for Government, serious concerns were raised about the value of one of these schemes—that a digital identity assurance scheme is itself vulnerable to criminal activity. What are the Government doing to ensure that that will not happen in this scheme?
James Brokenshire: We have seen, from some data losses in the past, the impact that this can have and, increasingly, as so many of our services move to an

online world, the need to have a trusted identity and identity assurance will continue to get more significant over time. In many ways, I think that is what lies behind the ID assurance solution that is being developed through this work. Clearly, privacy and security of people's identity is absolutely at the heart of this work, recognising the threats that I am sure will continue to be a challenge and that will continue to escalate. The work that is being undertaken is very much a core part of ensuring that our identities are protected, and the way in which services are designed will respect and reflect that. If we come back to what Mr Stringer said earlier about the role of Government, I think that this is very much part of it. The way that Government design their systems and provide that information assurance are a core part of what Government need to do in the design of their services and in taking more citizens into the online world.

Q76 Pamela Nash: I am not clear about this at the moment. I appreciate that it is still in a design stage, as you said, and that it will simplify the systems for customers—people who go online and access public services—and hopefully the aim is that it will be a more secure process for them. At the same time, an announcement by the Cabinet Office earlier this year indicated that a market would be set up to allow different private companies to get involved and to continue schemes.
James Brokenshire: It is interesting, because, if we look at information assurance, some of things that I have been talking about are as directly relevant to private companies and the way in which they set up their systems for facilitating business and for ensuring that customers are able to use their services as they are for Government in a number of areas. We envisage that the private sector will drive the solution, which is why there is this partnership approach in terms of the design process. The public sector will act as one of the early adopters of the system, in order to drive the standards and drive that approach, but, having got the design and got it right, we would see other businesses potentially adopting a similar sort of approach. The Government may be one of the lead adopters of the solution that is then designed, but then other businesses may take it on and utilise a similar approach, ensuring that the Government are doing their bit to raise the bar around information assurance in this arena.

Q77 Pamela Nash: Again, I have to highlight the fact that academics were very sceptical last week that business would take this on.
James Brokenshire: We are working very closely with business and industry around this particular piece of work. It is important. While there will always be those who are sceptical about particular pieces of work, raising the bar on information assurance and identity assurance is an important part of how we deliver a safer and more secure internet, given that so many more services are gravitating towards that area.

Q78 Pamela Nash: Could I ask you to expand a little on what you see as the benefits for individuals who are using the digital identity insurance scheme?
James Brokenshire: I suppose if you have a secure and trusted identity, it makes it easier to be able to use services, which ensures that people's experience of using online services is that much more effective. In some ways, it is about simplifying it so that it makes it more accessible and people are more readily able to use services online. If we are taking more Government services down that route, that is an important part of it. It is about that simplification, so that the public's ability to take advantage of online services is much more heightened. Simplification is one of the key things that the public will see, but ultimately it is also the safety, security and privacy building blocks that will sit behind it that will help to deliver on that overall framework.

Q79 Stephen Mosley: We have mainly been focusing on malicious software, but you can also have problems with legitimate software that has been poorly written because it could be exploited and people could take advantage of it. In the Home Office submission, you say, "We want the public and business to be able to identify easily products with good security. We will work with the private sector and others to identify how standards for measuring the effectiveness of products or services could be developed." Is that an aspirational statement or is there more meat on the bone than that?
James Brokenshire: One of the important issues around this is how we are best able to give that sort of information to the public so that they know what they are buying and the sort of assurance they are getting. One of the things that we are examining at the moment is whether the use of kitemarks and other such mechanisms is able to fulfil the basis of that statement. That work is very much ongoing. We are also working with CESG, which is at the centre of GCHQ and which does a lot of work on validation and certification, to see how best we are able to impart that assurance. It is not aspirational because work is ongoing on this to provide the information for the public on security and on assurance so that they are better able to know what they are buying.

Q80 Stephen Mosley: We heard about share value from one of the police officers earlier. Companies might not want to inform the police of problems that they have experienced because of shareholder value and because of the perception of risk to their brand. Do you think that that is a problem? If so and if companies are not declaring these things, do you think that there should be some sort of punishment or financial liability placed on them if they are supplying software or websites which they know are vulnerable?
James Brokenshire: This whole point of information assurance and of companies taking these issues seriously is a valid one. I made the point earlier about how we are able to take this from something that is viewed as being for computer experts to something that non-executive directors of companies are considering as very serious to their risk issues—issues of vulnerability and reputational issues—in relation to their businesses. There is legislation under the Data Protection Act to inform the Information Commissioner about data breaches and the rules and

requirements that operate there. This is something that we need to look at closely to ensure that we have good information about what is happening out there. If problems are emerging, it is something that I keep under consideration—whether regulation or some further step may be required—to ensure that that is being followed through and that we are able to get the information that law enforcement and indeed others would want to have to recognise threat and risk, or to make a prosecution, but equally to ensure the public are best advised about the risks that they may face if their data have been lost or mishandled in some way.

Q81 Stephen Mosley: The Government are probably one of the largest purchasers of software and IT services in the country. Do you use your own purchasing power to improve the quality of software that is out there?
James Brokenshire: We are doing that: the question is whether we can do more in the way in which we design services and, when we have new systems coming online, ensuring that security is very heavily rooted within that. That is something that Francis Maude takes the lead on in terms of procurement of IT services from across Government. Obviously, he heads up on cyber-security across Government as well. Therefore, when the Government buy services, software and systems, the safety and security of how we do that is a key element of the work that is ongoing. Do we need to do more? Yes, I think we do.

Q82 Stephen Mosley: Bringing all three strands together, if there was a company out there that you believed was not reporting things to the police, would you use your purchasing power to say, “No, we are not doing business with you”?
James Brokenshire: At the moment, it is getting the information so that it is clear in that way. I think what you are getting at is whether there are companies that perhaps have back doors or trap doors or something like that in the services that they are providing and what should happen. I would say that those companies would be running a significant reputational risk in the services that they provide in any event, and there are obviously liability issues that may reside around that and whether they are open to being sued for any errors in their software or their code that may be known and that they have not acted upon. There are a number of different ways to put pressure on those companies to up their game, although I am not aware that this is a significant issue in practice, from what I discern. Clearly, it is something that we will be keeping a close eye on.

Q83 Graham Stringer: The general perception is that the evil little geniuses who produce the malware, viruses and worms and things always get away with it. Do you think that that is a fair perception?
James Brokenshire: If what we are saying is that more people should be arrested and prosecuted, I agree with you—more people should be arrested and prosecuted, which is why we are investing in law enforcement and its capability as we are. This is something that crosses international boundaries, hence the reason for having that international link and, in many ways, for having the London Conference that the Foreign Office organised a couple of weeks back. I would also say yes, some of this is about organised criminals and those hackers who perhaps have been designing software as well, but it is also about the absurdity of the online, illegal supermarkets effectively offering software for sale to criminals, who may not be sophisticated. Therefore, when I talk about online or cyber-crime being a facilitator, that is one part that I focus on equally—how we are best able to disrupt, take down and bring those responsible to justice—because it is not always at that level of sophistication. People may be criminals without that technical expertise—they simply buy in illegal, black-market software to commit their crimes. There are a number of different levels of activity here. Some of the crime may not be considered and recorded as, for example, an offence under the Computer Misuse Act, but in fact be a traditional crime using a more sophisticated technique.

Q84 Graham Stringer: One of the police officers before was saying that they are focused on getting the Mr and Mrs Bigs and the gangs behind that. They tend to ignore the small-time criminal who uses software that he does not really understand and go for the bigger people. I inferred from what they said that they also could not get at the people who create the malware. I think you were agreeing with that point in what you said.
James Brokenshire: I certainly do not write off the criminals who are committing some of the crimes at the other end. You have the specialist capability that very much looks at the high-end work—the specialist technical work—but I want the strategic policing requirement and the establishment of the new cyber-crime unit, which is meant to better impart information and knowledge, to leverage and harness the response of police forces to crimes that are committed using technology. We need to ensure that we are doing both by mainstreaming our response to old crimes committed in a new way and by also looking at the more sophisticated end of the market.

Q85 Graham Stringer: Finally, is the legislative framework, or the legislation, that the police are working with at the moment sufficient? Does it need updating?
James Brokenshire: The Computer Misuse Act provides for offences relating to the creation of malicious software and to seeking to interrupt, disrupt or intervene in a computer system. We continue to keep the legislative framework under review. We are looking at how best the law enforcement agencies are able to operate. Clearly if there are gaps and if issues are arising—it was interesting, obviously, to hear the contributions in the preceding session—we will act on that as part of the work we are doing. Looking at the legislation and ensuring that it is fit for purpose is one of the key strands that we are undertaking. Equally, as so much of this crime is old-world crime, if I may describe it as that, we recognise the need to ensure that there is an understanding that many of the offences and much of the legislation is technology neutral and, therefore, it should not be seen that,

because it is in a new environment, there is automatically some impediment to charges being brought and prosecutions being made.

Q86 Chair: You will know that, from the prosecutions that were discussed earlier, many seemingly small crimes, as you put it, are actually conducted by people who have tentacles in very serious, high-level crime. This is a continuum with no hierarchical breaks—low-level petty thief up to high-level bank robber. This is a continuum and it needs to be managed in that way, doesn't it?
James Brokenshire: The individual victim of the crime certainly does not regard it as a small crime.

Q87 Chair: More than that, the criminals themselves travel up and down the spectrum. You do understand that?
James Brokenshire: I understand the point you are making. That is why I made the point about it not being a small crime. Any crime, if you are a victim of it, is appalling. If you are sitting in the safety of your own home and it happens to you, it is not acceptable.

Q88 Chair: Let's put it this way: it may just be a light-hearted point that the HMRC scam got through the House of Commons firewall this week, but, actually, behind that seemingly trivial crime there are serious, high-level players. Do you accept that?
James Brokenshire: There are victims here, first of all. I will labour the point because I think it is about understanding the real-life impact. I agree that there are organised criminal groups acting in this arena. That is why the National Crime Agency is configured in the way it is; it is looking very much at organised crime, financially motivated crime and border-related issues, as well as at the Child Exploitation and Online Protection Centre, with the cyber-crime unit being a capability that is available to those different strands. I think that is really important in the way this is configured, so that the very spectrum you identify is properly understood, and the intelligence hub that will be at the heart of the National Crime Agency will be able to interpret and understand that. Therefore, it is a coalescence of lots of crimes that in quantum terms may appear in isolation to be at a lower level in monetary terms—even though it will have a big impact on the individual, in isolation it does not involve millions of pounds. When you coalesce all of that together and gain that intelligence, you get a much clearer picture of the overall criminality being perpetrated, and about how it may well be organised or be international. We must therefore ensure that we gain that picture, so that the response is that much more effective.

Q89 Chair: A simple point. I am sure you will accept that e-commerce is increasingly critical to the UK economy. You heard evidence in the previous session about the relationship between the police and Nominet. Do you believe that we can do more to create a secure .uk domain, or do you think that that relationship is as good as it can be?
James Brokenshire: Our experience of the .uk domain is that it delivers a safe and secure domain. I think Nominet takes issues of cyber-security very seriously, and we are not aware of any particular problems concerning the .uk domain name being a significant problem in that sense. I know that where problems come up, Nominet treats them very seriously. We do not currently see the need for further regulations at this point in time, but obviously we will continue to keep the issue under review.

Q90 Chair: A few quick questions to finish. Ofcom investigates ISPs only when there have been repeat reports of bad behaviour. Are you satisfied with that, or do you think that the regulation covering ISPs should be strengthened?
James Brokenshire: At this stage we are not proposing to change the legislation or regulation. We prefer perhaps to build relationships with the ISPs to improve performance, and deal with the issue in that way. Obviously, we will keep the matter continually under review, but at this stage we are not proposing to change the regulation in that sphere.

Q91 Chair: In its evidence, PhonepayPlus told us that under its regulation, the UK enjoys the most "stable and sustained" premium-rate services in the world. Have you considered using it as a template for the regulation of e-commerce inside the UK?
James Brokenshire: It is not something that I am aware we are considering, Mr Chairman, but I am very happy to look at the evidence that was provided to the Committee and to see whether there is anything that might be considered.

Q92 Chair: Finally, I am sure that like everyone else in this room you have got a PC at home. Are you one of the 28% or not?
James Brokenshire: No, I do have software security on my home PC. I suppose it is about ensuring that we are all playing our part in that way. As I say, when I look at my role on UKCCIS—the UK Council for Child Internet Safety—it is about how we ensure that parents such as myself understand how all the filtering and the steps that we might want to take on our home computers are adopted appropriately, so that we are protecting ourselves as well as looking after our kids.
Chair: Thank you, Minister.
James Brokenshire: Thank you, Mr Chairman.

Written evidence

Written evidence submitted by the Home Office (Malware 00)

Prepared by the Home Office in consultation with other Government departments.

Introduction

1. This paper sets out the Government evidence to the Science and Technology Committee inquiry into malicious software (malware) and cyber crime. It has been prepared by the Home Office in consultation with officials from other Government departments including the Office of Cyber Security and Information Assurance at the Cabinet Office, the Cyber Security Operations Centre and the Department for Business, Innovation and Skills.

2. The paper outlines what the Government believes to be the situation regarding malware and cyber crime and makes references to current and future actions which are tackling these issues. Separate evidence will be submitted by the Serious and Organised Crime Agency (SOCA) and by the Metropolitan Police Service's Police Central e-Crime Unit. The papers from these organisations will provide more information on current operational activity to tackle cyber crime.

3. We define the term "malware" to denote software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system.

4. Malware allows criminals to compromise and control computers. This is achieved through a variety of means, including spam e-mails that encourage a user to click on a link that downloads the malware, or through placing malicious code in an otherwise legitimate website that will cause the user's computer to be infected when the website is viewed.

5. Malware is used for a variety of criminal purposes, in particular data theft. This might include credit card or bank account details, or industrial or government information, to be sold on for profit. Often the criminal and the purchaser of the information will be in different countries, with the victim in a third country.

6. We assess that the threat from malware is growing, with a huge rise in the amount of it being created and used—in 2010 more than 286 million unique malware variants were identified.[1] Some of these are relatively simple but many are highly sophisticated.

7. Of the various types of malware, Trojans have become the most prevalent—making up nearly 70% of attacks according to some anti-virus companies—as they are the most flexible in allowing the instigators of an attack access to the target computer. They can be seen as an enabler for all the other types of malware.

What proportion of cyber-crime is associated with malware?

8. Cyber crime falls into a number of categories, within the general principle that what is illegal offline is illegal online. Some crimes can only be carried out using the internet, including attacks on computer systems to disrupt IT infrastructure, and the stealing of data over a network using malware, often to enable further crime.

9. Other crimes have been transformed in scale or form by their use of the internet; for example credit card fraud can now take place on an industrial scale. Although crimes such as fraud and theft have always existed, the growth of the internet has opened up a new market, allowed for a degree of anonymity and has created new opportunities for organised criminal groups to finance their activities.

10. A third type of crime, which uses the internet but is not dependent on it, is that which is facilitated by the internet. Networks are used for communication, organisation, or to try to evade law enforcement, in the same way as older technologies such as telephones. The internet may 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. Mobile internet technology was used by rioters to co-ordinate looting and disorder in August of this year.

11. Determining the proportion of cyber crime which involves malware would therefore depend on which level of cyber crime was under consideration. Moreover, there is no easy measure of the levels of the different types of cyber crime or of how they operate. It is also difficult to gather and assess information on cyber crime as it occurs.

12. Work is being carried out to address this issue; for example, Action Fraud, which works closely with the National Fraud Intelligence Bureau, is to be expanded to become the single reporting point for financially-motivated cyber crime.

13. However, the threat posed by cyber crime is believed to be significant. *The Cost Of Cyber Crime,*[2] published by Detica and the Office of Cyber Security and Information Assurance in February 2011, estimates

[1] Symantec Internet Security Threat Report 2010

[2] http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

the cost to the UK of cyber crime to be up to £27 billion per year, or around 2% of GDP. Industrialisation of cyber crime to enable high volume activity, such as mass data theft, is largely reliant on malware.

14. It is therefore not possible to determine what percentage of cyber crime is facilitated by malware, but there is no doubt that it is a significant factor. As mentioned in the introduction, production of malware is increasing exponentially and it has transformed the ability of criminals to steal data over networks.

Where does the malware come from? Who is creating it and why?

15. The major threat from cyber crime comes from increasingly technically-proficient individuals and organised crime groups. These groups, and the infrastructure used in the attack, are often outside the jurisdiction of the UK. The criminals may be in one country and their means of cyber attack in a second and their victims in a range of other countries, making evidence gathering and identification of the criminals difficult. They may not fit the traditional profile of organised crime groups, and may be more of an affiliation of individuals who never meet except online.

16. Most organised criminal activity is aimed, either directly or indirectly, at making money. Organised crime groups and individuals use cyber technology to support traditional criminal activities or to develop new criminal schemes that exploit emerging vulnerabilities in rapidly evolving cyber technologies and online systems. By focusing their activity on areas which afford the broadest opportunities, criminals increase their potential monetary returns. Criminal finances and profits are central to organised crime and they constantly seek the opportunity to increase their returns whilst reducing their risk exposure.

17. Although most criminal activity is financially motivated, a spate of recent attacks on company websites has been orchestrated by activists protesting against those associated with ideals they disapprove of. This has highlighted the disruption that organised groups can cause, in order to further their aims, through the use of malware and techniques initially developed for other criminal purposes. This type of activity could be used against any public or private sector organisation with a presence online and against which a group may hold a grievance.

18. While the creator of malicious software may not be the end-user criminal, the goals noted above create a market place for malware. As such most of the malware writers will expect to profit from their works and have an increasingly sophisticated business model, including maintenance and support for their software, hiring their expertise out directly and upgrading their products in light of changes in the market, to support this. Malicious software and access to other tools, such as pre-existing botnets, is freely available for purchase at a variety of "underground" internet fora. This "underground" infrastructure also requires protection, leading to secondary layers of required technical expertise. The profit motive is less prevalent amongst the activist community where more ideological goals may drive the malware writers.

19. Many IT security companies report the source of malware as the location where it is hosted as it is often difficult to identify the origin of the software itself. This reporting of attack location rather than the source of the malware can badly skew statistics on where malware creators are based, however, the IT Security company BitDefender suggests in its H1 2011 report (http://www.bitdefender.com/files/Main/file/H1_2011_E-Threats_Landscape_Report.pdf) that China (31%), Russia (22%) and Brazil (8%) are the largest producers of malware.

What level of resources are associated with combating malware?

20. In October 2010 the National Security Strategy identified the cyber threat to the UK, which includes cyber crime, as a Tier 1 threat, on the same level as terrorism. £650 million of new money has been allocated to a National Cyber Security Programme 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 money will go towards enabling the UK to transform our response to cyber crime, of which countering malware is an important element. This money is additional to the resources already allocated to the police and other agencies to tackle crime, including cyber crime.

21. The NCSP will also bolster cyber capabilities within the intelligence community. GCHQ, as home of the National Technical Authority for Information Assurance, CESG, is of particular relevance here. CESG's role is to provide consultancy and technical support to government and others, in order that they are able to understand the risks they face and can therefore protect vital information services and data. Improving protection of data through reducing vulnerabilities via which malware can gain a foothold is key to reducing the effectiveness and impact of the malware, and can be much less costly than taking a reactive stance whereby malware is only identified after it has had a detrimental impact.

22. The Police Central e-Crime Unit (PCeU) and the Serious Organised Crime Agency (SOCA) include the combating of malware as part of their current work on tackling cyber crime. Further information will be provided in their own evidence to this enquiry.

23. Work has begun to create a dedicated cyber crime unit as part of the National Crime Agency, building on the work already done by SOCA and PCeU. There will continue to be close working between the two units to develop the national response to cyber crime in advance of the creation of the NCA. This will be a specialist unit and will support the work of all of the commands within the National Crime Agency.

24. The unit will be the national centre of excellence for law enforcement, and will provide resources, intelligence and guidance on best practice to forces. To support the mainstreaming of knowledge of cyber crime, the learning developed by the unit will be fed into police training programmes to provide understanding of online crime issues across the police service.

25. In February 2011, the Prime Minister brought together 13 CEOs from a broad spectrum of large companies to discuss private sector resilience to cyber threats, including online crime. The meeting was designed to inform them of our new approach to tackling this issue and the renewed emphasis on improving the UK's cyber security capability, including better protection for business from all types of online threats and the need for the private sector to work in partnership with government to achieve this aim. At that meeting it was agreed that a joint capability, in the form of a "hub", would be co-designed by a cross sector working party.

26. Since then, the working group has been meeting regularly to turn the "Hub" into reality. The group will report back to the Prime Minister in the autumn and an announcement will be made on the manifestation of the Hub, calling on all organisations to take an active role in protecting our collective interests in cyberspace.

What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

27. Cyber crime causes harm to individuals and the private sector in a range of ways. It results in direct and indirect financial losses amounting to billions of pounds, adverse credit ratings and protracted disputes over suspect payments, and causes damage to reputations. Further harm can be caused by online extortion, bullying, harassment and hate crimes.

28. The Detica/ OCSIA *Cost of Cyber Crime* Report estimated that the cost to citizens of all types of cyber crime taken together (not just that involving malware) was £3.1 billion per annum. The loss to industry, including from intellectual property theft and espionage, was estimated at £21 billion.

29. We are aware of some excellent initiatives that have been taken by internet service providers to combat the spread of malware. These include initiatives such as anti-virus alerts when visiting websites and warning customers whose PCs are part of a botnet.

30. The banking sector has also invested heavily in ID assurance products for online banking customers, as well as providing free software for internet users which monitors transactions and alerts when malware is detected on a system.

31. Such innovation is welcome and shows what can be done when the private sector tackles security issues in partnership with consumers. However, we believe that more could be done.

32. The government plans to discuss with the largest internet service providers a possible partnership between industry, government and law enforcement to establish how malware and botnet activity on the networks could be identified and addressed.

33. We also want to make sure that the public and businesses understand the risks of being on line and know how to take the appropriate action to protect themselves. Get Safe Online (www.getsafeonline.org) is a joint initiative between the Government, law enforcement, business and the public sector, which has been created to provide computer users and small businesses with free, independent and user-friendly advice to help them to use the internet confidently and securely.

Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?

34. The Government is committed to tackling the security challenges we face in cyberspace, which include the pervasive distribution of criminal malware. However, taking action to prevent cyber crime cannot be the responsibility of the Government alone. The private sector and the public have important roles to play alongside law enforcement organisations, technical experts within government departments and the intelligence and security community.

35. Keeping security software and operating systems up to date and running anti-virus programmes are two key methods to reduce the risk of computer systems being compromised by malware. A major contribution to reducing the vulnerability of systems to cyber crime can come through industry's ability to deliver consistent, good quality information assurance products and services.

36. This can range from a member of the public choosing an appropriate security package to install on their home computer, to a large organisation designing its online services securely. We want the public and businesses to be able to identify easily products with good security. We will work with the private sector and others to identify how standards for measuring the effectiveness of products or services could be developed.

37. Much has been done to raise awareness of online threats, including through the website Get Safe Online. We will build on that initiative and others by developing a single Government portal for the provision of advice on internet safety to the public and businesses. We will ensure that the information gathered by law enforcement and the private sector which might help internet users is shared. We will drive this by making sure that every Government website, as well as DirectGov, contains a link to this safety information.

38. In this respect, the approach we are taking to combating malware is similar to how the Government approaches the control of human disease, being a multi-stakeholder approach which looks at the problem holistically, resulting in a number of policy options to tackle the creation and distribution of malware in parallel to mitigating the damage caused and bolstering defences. In addition, in some circumstances infected systems may also be quarantined.

How effective is the Government in co-ordinating a response to cyber-crime that uses malware?

39. By building upon existing capacity within the intelligence and security agencies and law enforcement units the Government is investing in better protection against malware and increased disruption of criminal networks. Further information about ongoing activity to combat malware and cyber crime will be provided by SOCA and PCeU in their evidence to this enquiry.

40. The Government has been proactive in identifying cyber crime and the proliferation of malware as a key international security issue. As such this issue will form a core element of discussions at the London Conference on Cyber Space in November, hosted by the Foreign Secretary, which will bring together representatives of over 60 nations and international organisations.

41. The Government has also been instrumental in working more closely with the primary victims of malware and online crime, the private sector. Millions of UK citizens rely on secure online systems for their livelihoods as well as underpinning their enjoyment of the online world. We increasingly shop, communicate, transact and interact socially online. Confidence in the security of the internet is therefore critical to consumer confidence.

42. With this in mind the Government's collaboration with the private sector has progressed to form a lasting partnership to improve our collective response to cyber attacks on both public and private sector systems. This work will continue with the intention of creating a mechanism to share actionable intelligence on cyber threats, including malware, between Government and the various at-risk areas of the private sector.

43. The Government has recognised that we need to do more to respond effectively to cyber crime. We will shortly publish our cyber crime strategy setting out how we will achieve a transformation in our approach, supporting activity across all sectors—the public, business, Government and law enforcement—to deliver an integrated response.

44. We will reduce the vulnerability of the UK through better system design, crime prevention and public awareness; reduce the threat to the UK through disruption and prosecution of online criminals; and reduce the impact on the UK through the development of partnerships with the public, business and international partners.

7 September 2011

Supplementary written evidence submitted by the Home Office (Malware 00a)

LETTER TO THE CHAIR OF THE COMMITTEE FROM JAMES BROKENSHIRE MP,
PARLIAMENTARY UNDER-SECRETARY OF STATE FOR CRIME AND SECURITY, HOME OFFICE,
28 NOVEMBER 2011

Thank you for the opportunity to give evidence to the Science and Technology Committee's enquiry on malware and cyber crime. I welcome the Committee's engagement in considering ways of tackling this increasingly important issue and look forward to your report.

I undertook to write regarding the question of progress on the Identity Assurance programme. The programme, which sits within the Government Digital Service and is led by the Minister for the Cabinet Office, Rt Hon Francis Maude MP, is working with departments to develop a federated identity assurance model. Ms Nash raised the question of whether the programme was on schedule, as she believed a prototype was to have been tested in October.

I am happy to confirm that, in line with the stated schedule, a prototype was made available in October, in the form of a Beta solution developed by the DWP Universal Credit programme. This sought to prove various technical aspects of the proposed architecture, and was successfully tested with a number of potential private sector Identity Service Providers. The wider cross-governmental solution is now being reviewed and further developed following feedback from the commercial sector.

It might be helpful for me to provide some further information about the purposes of the scheme. The Identity Assurance programme deals with the way a service provider can be assured that the customer or user is who they say they are as they access Government services. The user will be able to choose an identity assurance service from a range of certified providers; the user may choose to register for one or many of these services. The model will place the user in control. The user will determine how his or her personal data is disclosed when registering to create a digital identity and subsequently when the digital identity is used.

A principal difference with the now defunct National Identity Scheme is that it discards the reliance on a central identity register in favour of a decentralised, federated structure. Public service providers will determine the level of identity assurance they require; the user will then meet those requirements using an identity provider.

The Identity Assurance Programme is working with Industry, the National Fraud Authority, National Fraud Intelligence Bureau, Serious Organised Crime Agency, CESG (the UK's National Technical Authority for Information Assurance) and other interested stakeholders to ensure the design has appropriate capabilities to combat fraud, protect the user's privacy and enhance the customer experience of digital transactions.

The programme supports the "digital by default" policy. Digital transactions offer both convenience for customers and cost saving opportunities for public service providers. For the model to be successful there must also be benefits for commercial identity service providers. The programme's commercial workstream is working with industry to develop suitable commercial models.

Mike Bracken (Executive Director of Government Digital Service) took over as SRO for the Identity Assurance Programme at the beginning of October. Funding for this programme has now been agreed and a review of the existing programme and associated resources will be undertaken and completed by the end of the year.

Our ambition is for this programme to create new private sector enterprise, new investment, more jobs and ultimately produce trusted solutions, which will be key to ensuring citizens have greater confidence to engage with public (and private) sector services online.

I hope this will reassure the Committee about the progress of the programme and the importance of this work to improving the security and accessibility of Government services.

James Brokenshire MP
Parliamentary Under-Secretary of State for Crime and Security
Home Office

November 2011

Written evidence submitted by Professor Peter Sommer (Malware 01)

1. I am a Visiting Professor at the London School of Economics and a Visiting Reader at the Open University. I have acted as an expert witness in many trials involving complex computer evidence; some of these have included the deployment of malware.

2. The Committee will recall that I provided written and oral evidence for its earlier inquiry into Scientific Advice in Emergencies (HC498).

3. As an academic I have had a very long-standing interest in the issues of the statistics of computer-related or "cyber" incidents as these are often used as the basis of formulating security policies. 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. I believe I may be able to assist the Committee by drawing to its attention the problems associated with defining "cyber-crime", producing statistics of its incidence and providing measures of harm or damage.

5. **Declaration**. I have no commercial links to any organisations offering products and services dealing with malware.

Definitions of Cyber-Crime

6. There is no generally-agreed definition of cyber-crime and this lack directly impacts assessments of extent. We can illustrate the diversity of definitions. The Council of Europe CyberCrime Convention,[3] 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". It will be seen that articles 4 and 5, respectively, "data interference" and "system interference" include "malware". 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."

7. 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*,[4] 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[5] and the report excludes any direct reference to malware or to child pornography.

[3] 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.

[4] http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

[5] http://www.justice.gov.uk/lawcommission/docs/cp150_Legislating_the_Criminal_Code__Misuse_of_Trade_Secrets_Consultation.pdf

8. The Committee will need to be alert to "research" the main aim of which is to sell product and services rather than inform about risk. The Committee should also watch carefully for the use of language that scares rather that informs. At the moment a number of malware vendors are referring to something called "Advanced Persistent Threats" or APTs. At any point in the last 40 years of computer security there have been threats which for their time were "advanced" and which were deployed with "persistence". Whilst some malware can be readily and usefully identified by way of their methods of exploitation or distribution—for example "buffer overflow", "cross-site scripting", "back-door", "boot-sector", USB autostart", "browser hijack", "covert registry modification", "email address book hijack" etc, "APT" appears to have no useful meaning.

Estimates of Cyber Crime

9. Most official forms of crime recording in the UK are on the basis of specific offences prosecuted. But in relation to "cyber crime" there are particular difficulties as a result of policies of the Crown Prosecution Service. It sees the 1990 Computer Misuse Act as designed to fill in gaps in other forms of legislation[6] 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. The keystroke monitor would be classified as "malware". 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 malware "back doors") would probably be charged as extortion as this is the most common way in which criminals can make money. In every year since the Computer Misuse Act came into force, prosecutions have seldom exceeded 100 per year.

10. As with many other studies of the extent of crime there are significant methodological difficulties—how far does one include crimes which are suspected but never come to court—what should be the standard of proof for inclusion? Is this "proof" the act of reporting to the police or replying to a question in a survey? What fudge factors should one apply for situations where individuals *think* they have been subjected to criminal actions but have not—or where they have actually been victimised but have an inadequate realisation? What further fudge factors do you allow for unreported crimes? In relation to activities which cause distress, do you only include situations where a crime has been committed?

11. In terms of the incidence of malware, the problems of collecting data are somewhat easier. A number of anti-malware vendors offer out-sourced services. The customer agrees to route all his email and web traffic via the vendor who then detects and removes the malware. In an alternative, the customer installs on his own premises a "black box" controlled by the vendor which has the same effect. In both instances the anti-malware vendor is in a position to collect statistics about the variety and frequency of deployment of malware. Examples of such statistics come from Symantec,[7] Macafee,[8] Sophos[9] and Websense.[10]

12. However these statistics are not reliable as to harm and impact. They refer to situations where malware has been detected and, for the most part, thwarted. They do provide a powerful argument for deploying anti-malware products.

Financial Costs of Cyber Crime and Malware

13. The cost of any incident can be divided into direct and consequential. Direct: "My building and contents have been destroyed and I need money to replace them". Consequential: "While waiting for the replacements I was unable to generate turnover and profit". In the vast majority of malware-triggered incidents there is no physical damage, so that all the losses are consequential. As such the extent of loss in any one incident is substantially a function not of the malware itself but of the use to which the affected computer is being put and the speed with which the victim can recover. That in turn reflects the existence and efficacy of a contingency plan. Contrast the positions of a PC used domestically for entertainment hit by the same malware as a PC sitting on the desk of an city financial trader dealing in multi-million dollar contracts.

14. A further issue is what to include in remedial costs—what allowance do we make for imprudent victims who have not taken elementary precautions to protect themselves—or who through clumsiness actually make the situation worse?

15. For this reason all estimates of the costs of cybercrime and malware are wildly speculative.

16. Some analysts seek to include "lost business opportunities" as opposed to a loss of revenue. The latter can be established by extrapolating from the past business records of a victim and is insurable, the former is simply an optimistic guess and is not insurable. Returning briefly to the BAE/Detica Report mentioned above:[11] At page 3–6 "Costs of different types of cyber crime to the UK economy" identifies "IP Theft" at

[6] Statements frequently made by CPS officials in public and private

[7] http://securityresponse.symantec.com/business/threatreport/topic.jsp?id=threatreport&aid=notable_statistics

[8] http://home.mcafee.com/VirusInfo/RegionalVirusInformation.aspx

[9] http://www.sophos.com/support/knowledgebase/article/58736.html

[10] http://www.websense.com/content/threat-report-2010-introduction.aspx

[11] http://www.detica.com/uploads/resources/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf

over £9.2 million and "Industrial Espionage" at £7.6 billion. At page 5 there is a table purporting to break down "industrial espionage" losses by industry. It is difficult to see by what plausible methodology these figures were obtained. AS we have seen, the Report does not cover malware at all.

17. Statistics and cost impacts are a valuable aid to policy making but reliance on invented figures can only result in bad decisions.

18. Looking specifically at malware, provided that potential victims subscribe to a high quality anti-malware products which pick up the overwhelming majority of threats, the main impact is the cost of the subscription to the service. For domestic users free anti-malware products are available, eg Grisoft AVG[12] which incur no cost at all. This would leave the impact of so-called zero-day malware, that is malware which has not to that point come to the attention of the anti-malware vendors and is not detected by their products. As we have seen above, loss is then a function of where and how a specific computer is being used and associated contingency / data recovery plans.

Responses to Committees Specific Questions

Q1. *What proportion of cyber-crime is associated with malware?*

19. Please see my paragraphs 6–12 above.

Q2. *Where does the malware come from? Who is creating it and why?*

20. This is not directly within my expertise. However it appears that there are several different motives. A distinction needs to be made between malware which is released generally and malware which is specifically aimed and where it is part of a targeted act to cause harm, or create opportunities for fraud, espionage or extortion. In the former, the aim seems to be to prove the "success" of the exploit by the number of infections and is essentially a technical challenge; it is a variant of recreational hacking. We can divide targeted exercises as ones aimed at specific individual persons or companies for immediate effect in terms of causing harm; and "harvesting" activities where the targets are initially indiscriminate but the aim is to acquire username/ passwords and other credentials which can later be used to carry out a fraud or similar.

21. Much malware is possible because of the increasing complexity of modern operating systems and applications and their release by software houses without proper testing. Companies like Microsoft desire the additional revenue that the frequent release of new software versions bring and then offer to remedy discovered faults, post purchase, by the provision of frequent "patches". But what other product in history issues rectifications once a week for its entire life-cycle as is the case with its main operating systems? The product faults are discovered by the computer security research community and these are then turned, often by others, into the exploits that become malware. Government could use its power when buying operating systems and application programs and complain about the high level of exploitable bugs.

Q3. *What level of resources are associated with combating malware?*

22. The main resource is that of that anti-malware companies who discover new instances and then include detective and remedial measures in their products. All businesses need to have a contingency/recovery plan to cover a variety of scenarios, including malware infection. Such plans are a combination of data back-up and management action plans. See also my remarks at paragraph 25 below about policing.

Q4. *What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?*

23. See my remarks at paragraphs 13–18 above.

Q5. *Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?*

24. This appears to be a misleading analogy as there is no equivalent for malware for the doctors, nurses and hospitals which make up the NHS nor any need for them. The main remedies are anti-malware products and contingency/back-up plans. There is an argument for a modest publicly funded Computer Health Information Service which includes advice on malware and contingency planning. This role is fulfilled by GetSafeOnline though there are questions about its level of funding. But much of the effort could surely be left to the private sector anti-malware vendors, whose interest in this instance in selling good products aligns with the national interest in protecting the public and business.

Q6. *How effective is the Government in co-ordinating a response to cyber-crime that uses malware?*

25. For malware that is released but not targeted the main aim of Government policy should be advisory—see my remarks above. For malware used as part of a targeted criminal process the additional remedy is effective policing. The same police resource could also be used to identify those very few UK-based instances

[12] http://free.avg.com/us-en/free-antivirus-download

where non-targeted malware is authored or deliberately released from the UK, for example Christopher Pile, sentenced in 1995 at Exeter Crown Court. The Committee will be aware of the current confusions and uncertainties surrounding the policing of e-crime in the UK. The main unit is the Police Central E-Crime Unit based at the Met. The new National Crime Agency will incorporate many of the features of SOCA, the Serious Organised Crime Agency, which has a e-crime unit, the investigation of frauds, the commission of which may involve malware, is the remit of the City of London Police. If malware, in the form of backdoors and keystroke loggers is used in espionage attempts this would presumably be a role for the Agencies. The Centre for the Protection of the National Infrastructure (CPNI) has a role in advising government departments and businesses with key government contracts of threats and measures in general including, presumably, malware. It would be helpful if the Committee is able to highlight duplications and uncertainties of scope of remit between these various entities.

I would be happy to expand on any of these issues.

5 September 2011

Written evidence submitted by Intellect (Malware 04)

I am writing to offer Intellect's formal submission to the House of Commons Science and Technology Committee Inquiry into Malware and Cyber-crime.

Intellect is the UK trade association for the IT, telecoms and electronics industries. Its members account for over 80% of these markets and include blue-chip multinationals as well as early stage technology companies. Our diverse cyber security portfolio reflects the fact that the technology industry has a critical role to play in the drive to online security, including providing agile solutions to cyber threats, supplying intelligence on attacks on information systems and in protecting itself, as part of the national infrastructure, from these attacks.

While a number of Intellect's member companies are submitting full written evidence to this inquiry, we have chosen to highlight below the issues most salient to the technology industry:

- Malware is becoming an increasingly common means of attack for cyber criminals and is often combined with sophisticated social engineering tactics.
- A shadow economy in criminal IT services has emerged and is largely driven by organised crime. Those targeted for attack range from individuals, private companies, national infrastructure and nation states.
- Estimating the cost of cyber-crime is problematic. Many private sector organisations are unwilling to publicly announce either breaches of their IT systems or their security spend for fear of reputational damage.
- Companies within the technology industry must share information on threat data in order to ensure comprehensive cyber security.
- There is a conceptual flaw in organising response actions along an artificial distinction of the public and the private that the perpetrators of cyber-crime do not recognise.

Intellect is developing a number of projects to address some of these issues, such as an information-sharing forum and a cyber security best-practice guide for small businesses and I would be very happy to formally brief the committee on these activities.

Gordon Morrison
Intellect Defence and Security Director

5 September 2011

Written evidence submitted by Dr Richard Clayton (Malware 10)

1. I am currently a Senior Research Assistant in the Computer Laboratory of the University of Cambridge. At present I am engaged in a three-year collaboration with the National Physical Laboratory (NPL) to develop robust measurements of Internet security mechanisms.

2. I have a particular research interest in cybercrime. My research falls mainly under the heading of Security Economics—a field based on the premise that it is easier to explain security issues with an economic analysis rather than simply using a technical or "computer science" approach. I am particularly interested in measuring criminal activity rather than merely describing it.

3. I have been using the Internet since the early 1990s, ran a software house that created one of the earliest mass-market Internet access products, and worked at Demon Internet, then the largest UK ISP, from 1995 until 2000. In October 2000 I returned to Cambridge to study for a PhD. My doctorate was awarded in January 2006 for my thesis, "Anonymity and Traceability in Cyberspace".

4. I have continued to work in the Computer Laboratory doing academic research. On several occasions I have acted as specialist adviser to House of Lords and House of Commons Select Committees in inquiries into cybercrime and Internet security.

5. I have written, or co-written, over 40 peer-reviewed professional publications. My main research interest over the past few years has been into the criminal activity called "phishing"—the theft of financial credentials by impersonating legitimate websites. More recently I have been starting to look at the role of malware in the criminal eco-system and I have published work on how malware clean-up should be approached from a security economics standpoint.

6. I should also declare that in addition to my employment at Cambridge and my past association with Parliamentary Committees, I am a director of a small consultancy company that sells my time and expertise. Additionally, I am presently employed by Yahoo! in a part-time capacity within their security team.

7. This document expresses my personal opinions, and is in no way the expression of an official position held by the University of Cambridge, NPL, or Yahoo!

Q1. *What proportion of cyber-crime is associated with malware?*

8. I have been pointing out for years there are almost no reliable figures about cybercrime. In a report I wrote with colleagues for the European Network and Information Security Agency (ENISA)[13] we set out the problems in detail in section #4.2.

9. Summarising 14 pages of densely argued analysis for this submission is impossible, but in section #4.4 we made two recommendations, both of which I would commend to this Committee:

We recommend that the Commission (or the European Central Bank) regulate to ensure the publication of robust loss statistics for electronic crime.

We recommend that ENISA collect and publish data about the quantity of spam and other bad traffic emitted by European ISPs.

10. Until we have reliable data we will not be able to assess the size of the cybercrime problem nor whether we are making any impact on it. Of course, assessing that impact in purely monetary terms is simplistic and the Committee ought to go beyond what we recommended to ENISA and require the recording of all electronic crime incidents, not just those resulting in monetary loss.

11. For example, the UK banking industry already publishes fraud loss figures—but these do not actually document how much money has been stolen, but rather how much the banks end up out of pocket. The bank has no loss if they detect the crime promptly enough to undo electronic transfers before the money leaves the banking system (which we understand is achieved in about half of all cases).

12. Additionally, banks regularly attempt to dump their losses onto their customers, personal and business, by suggesting that the failure of security mechanisms is the customers' fault, despite those mechanisms having been specified by the bank.

13. In particular, to return to this inquiry's focus on malware: banks and others have chosen to rely on general purpose browsers and they have chosen to rely on identifying users simply by their ability to regurgitate a password. Unfortunately, when user machines are infected by malware this reliance is misplaced.

14. Most modern malware includes a "keylogger"—functionality to record all the keystrokes typed by the user and relay them to the attacker. In response, the banks have moved to systems that prompt on the screen for just a few characters from the password. There is now malware that snaps a copy of the screen area around the mouse and the criminal learns the password one character at a time.

15. More sophisticated software performs "man-in-the-browser" attacks by intercepting legitimate interactions with the bank—perhaps paying a gas bill—and replacing this request with a transfer of money to the criminal's account.

16. This type of malware operates in "real-time" and will defeat the protection provided by the "CAP readers" (the calculator-like devices that many of the banks have issued). This is because the user will type in the numbers from the screen still believing that they are paying their gas bill. Even after the fraud is complete the malware will keep the user from realising they have been defrauded by rewriting onscreen bank statements to continue the pretence of paying for gas.

17. One could carry on for many pages in discussing numerous different types of malware and explaining all the different types of criminality that it underpins. Unfortunately, this descriptive approach is pretty much all that we have—we have almost no reliable quantitative information.

18. Hence it is not really possible for anyone to give an accurate answer to the Committee's specific question about the proportion of cybercrime that is associated with malware. All that can be said, in the most general terms, is that the eco-system for mass-market criminality is based on spam sent by botnets, and those botnets

[13] R Anderson, R Boehme, R Clayton, T Moore: *Security Economics and the Internal Market*. ENISA, Jan 2008. http://www.enisa.europa.eu/act/sr/reports/econ-sec

are constructed by compromising end-user machines with malware. Furthermore, the majority of specialist attacks on high-value targets—performing industrial espionage or compromising finance departments—are also based on malware.

Q4. *What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?*

19. The committee asks a number of questions about malware authorship and the cost of protection which other experts will be able to address. What I can discuss, from my own research, is the ineffectiveness of protection—and, rather unusually, I even have some detailed numbers about this relating to the activities of one particular criminal gang.

20. First some generalities. Systems such as spam filters act to protect individuals by preventing them from ever coming into contact with malware. However once an email evades those filters and arrives in the inbox with a malware attachment or a link to a bad website then there is almost no further protection at all. Of course some people will see through the "social engineering" and will not be fooled into clicking the malware into action, but now that the criminals understand what is too enticing to ignore (and now they have fixed all their grammar and spelling errors) clicks are extremely common.

21. I have spent the past year tracking "Instant Messenger worms"—malware that is spread between Instant Messenger buddies. What happens is that users receive a message over Skype, Yahoo! Messenger, Microsoft Messenger, Facebook Talk etc. which says something like:

foto http://ofacebooks.net/album.php?your@email.addre.ss

22. If the user clicks on the link in this message then Windows will put up a warning message asking whether you wish to run a program from ofacebooks.net. Most people, I believe, are so eager to see the promised photograph that they will immediately press OK and thereby become infected by the malware.

23. Once the malware is running on a new machine it contacts its command and control system (C&C) to determine what it should do next. The C&C will generally instruct it to send a message to all of the new victim's buddies (saying foto… etc) to garner new recruits. The C&C will then download specialist malware (keyloggers, vulnerability scanners, spam senders, etc) and the machine will be mined for financial data and turned into a resource in a botnet.

24. At the time of writing, my research shows that the malware for the most active worm is being downloaded just over 70,000 times a day and the number of victims, worldwide, is now well into the millions. This research is currently unpublished—but I expect it to be of significant import, not least because for once we have some accurate numbers to work with.

25. One might expect anti-virus software to detect the downloaded malware and hence provide protection. However, the criminals tweak the malware on a daily basis and only deploy it once it is passed as safe. Then of course the anti-virus software is updated, but too late to protect anyone.

26. To take just one example of the how ineffective anti-virus software is: consider the specific version of the malware that the criminals were using between 10:27 and 14:23 GMT on the 5 September. It was tested at 16:54 (90 minutes after the criminals stopped deploying it) and by that time it was detected by only seven of 44 anti-virus products; and those seven did not include any of the top three products by market share. Even 24 hours later, only 11 products reported this particular malware sample to be bad.

27. Of course, not all malware gets onto people's machines because they click on a link and are "socially engineered" into ignoring warnings. Some infections result from exploiting software bugs—for example in the add-ons that automatically play videos within the browser.

28. The large software companies such as Microsoft and Adobe provide automated patching systems to correct bugs. However, modern computers are running software from dozens, if not hundreds, of companies—and most of these companies do not have sophisticated patch distribution mechanisms. It would be desirable for companies such as Microsoft to open their patching platforms to third parties so that users could have a fully integrated way of staying up-to-date.

29. Other companies are just as slow at deploying patches, and in particular the mobile phone companies can be years behind at pushing out patches to their subscribers' handsets.[14] This is a classic failure that is easily explained by "security economics": the people in a position to fix the problem are not those who would suffer a loss. We often have to resort to fixing such problems by regulation—and this Committee should recommend that subscribers should be entitled to claim damages from their network provider if their phone (or their data) was damaged as a result of an unpatched vulnerability for which they have delayed rolling out a fix.

[14] R Lemos: Fast phone patching still a fantasy. CSO Magazine, 7 April 2011. http://www.csoonline.com/article/679205/fast-phone-patching-still-a-fantasy

Q5. *Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?*

30. Another way that industry fails to protect Internet users is by failing to act when their users are known to be compromised.

31. It is often possible to record the unique IP addresses of machines that are contacting a C&C system. Additionally, when a botnet is shut down it is now usual practice to set up a “sinkhole” that will log the identities of the compromised machines which continue to try and make contact with the disabled C&C.

32. The operators of the sinkhole are unable to communicate with the owners of the compromised machines directly—they can only identify the ISP that is providing Internet connectivity. So it is up to the ISP to pass the bad news on to the relevant customer, because only the ISP knows who was using the IP address at the relevant time. In practice very few ISPs relay information and almost none go looking for further sources of this type of data.

33. We can see how poor the data passing is by examining the data collected by the Shadowserver Foundation, who operate a sinkhole for Conficker—malware that infected seven million machines worldwide in November 2008 and which still poses a threat to the infected machines. The Shadowserver data[15] shows that infections have dropped from 5.5 million in September 2010 to 3.5 million now; the worst affected UK ISP has seen a reduction from 7000 to 5000 infected machines over the same period. The best ISPs completely eradicated the problem, and ensured their customers were safe, two years or more ago, and I suspect that the drop in numbers is as now much to do with old computers being scrapped as customers being told of their problem.

34. The reason that ISPs discard notifications is because contacting their customers is expensive—the standard meme is that one phone call to a customer wipes out the profit made on them for a year. This makes a good sound-bite—but it is roughly correct. My own analysis shows that the cost equates to eight months of profit, so the ISPs are indeed acting rationally in so far as their own self-interest is concerned.

35. Financial concerns are the basis of the industry-wide agreements (in Germany, Australia and The Netherlands) in which all the ISPs promise to pass on malware infection notifications. The idea is to ensure that no-one can steal market share by undercutting prices by failing to incur the cost of contacting customers.

36. This committee should recommend just such an ISP industry-wide agreement in the UK. However, the recommendation should go further and instruct the ISP industry to explicitly seek out sources of data, from sinkhole operators and others, so that UK Internet users have the best possible chance of being told if their machines are harbouring malware.

37. The Committee should pay particular attention to the system being operated by Comcast—the large cable provider—in the United States. They monitor traffic to their domain name servers—the machines that convert human-memorable hostnames into the IP addresses needed to communicate across the Internet.

38. Comcast use a datafeed from Damballa, a specialist anti-malware firm, to identify when hostname lookups are performed by malware that is attempting, for example, to locate C&C servers. When the presence of malware is deduced then the customer is informed, usually by means of a pop-up message when they next use their browser.

39. One of the many reasons that ISPs fear talking to customers about malware is not just that they want to avoid delivering bad news, but they fear being pressured into having to explain all of the detail—and then being roped in to fix the problem. What Comcast have done to avoid this is to provide substantial online help and links to free online clean-up tools. Further, they have done a bulk deal with a specialist company who will, for an $89.95 fee, give personal help to customers.

40. I considered the economics of this type of clean-up operation in a paper that I presented to the Ninth Workshop on the Economics of Information Security in 2010. This peer-reviewed conference is the leading forum for work in the Security Economics field. A slightly revised version of the paper was subsequently published in Volume 81 of the Communications & Strategies journal.[16]

41. My paper,[17] “*Might governments clean-up malware?*” supposed that the government would subsidise the cost of malware clean-up, and modelled what the costs might be. I considered a world in which ISPs passed problem reports on to their users, but if the user could not fix the problem they would be referred to a standard clean-up service. The users would pay a nominal sum ($30 (£20) perhaps) to avoid any moral hazard, and the government would subsidise the rest.

42. The thrust of my argument is that this is not as expensive a scheme as it might at first appear because the contractor would be able to sell other services off the back of their interaction with users. Hence they would swallow some of the subsidy costs themselves in order to land the government’s contract. My modelling

[15] http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker

[16] R Clayton: *Might governments clean up malware?* Ninth Annual Workshop on Economics and Information Security (WEIS10), Cambridge MA, US, June 7–8 2010.
R Clayton: *Might governments clean up malware?* Comms & Strategies, 81, 2011, pp. 87–104.

[17] http://www.cl.cam.ac.uk/~rnc1/malware.pdf

suggests that the actual cost for such a scheme would be less than £0.50 per citizen per year—comparable with the costs of fluoridising the water.

43. There are of course numerous details and assumptions in this scheme, and I refer the Committee to the full paper for all of the details, and a discussion of the advantages of involving the government in such a scheme. The Committee might also note that the German malware clean-up initiative[18] is partially funded by the German government.

Q6. *How effective is the Government in co-ordinating a response to cyber-crime that uses malware?*

44. The government has not dealt with cybercrime effectively, whether it involves malware or not. Successive administrations have failed to provide adequate funding to grow and develop the specialist police units who work in this area. A very small number of officers have practical experience of tackling cybercrime and this has given them a rarity value in the job market, so that personnel retention is a significant issue.

45. The Committee should be recommending more resources—if only because cybercrime is volume crime that affects very large numbers of citizens. We have (a rarity as ever) some good data on credit card fraud, much of which is Internet related. A supplementary document to the British Crime Survey was published by the Home Office in May 2010. It looked at data from 2008–09 and found that 6.4% of credit card owners were aware of fraudulent use of their card over the previous 12 months. Victimisation rates were higher at 11.7% for incomes over £50,000/annum. If the Internet had been used at all (irrespective of income) the rate was 7.7% and if the Internet was used "every day" then it was 8.9%. In contrast, the 2010–11 British Crime Survey found that burglary affected just 2.6% of households and thefts from cars affected 4.2% of households.

46. There has also been a complete failure by government to even start to address the need for effective international responses to cybercrime. Police work needs to be coordinated at the international level, because otherwise committing a crimes in another country will make you untouchable.

47. In the US when 1930's bank robbers used the new-fangled automobile to flee across state lines, the solution was to make bank robbery (along with auto-theft and other related offences) into federal offences rather keeping them as state-specific infractions. However, this solution does not look to be practical for cyberspace, because there is no global body with the equivalent reach over the world's countries that the US federal government had over the individual US states.

48. We are not going to see cyber-police operating across borders in the near future, but we should be looking to see substantially more international cooperation in pursuing criminals in one jurisdiction who have committed crimes in another.

49. The best solution that I and colleagues have been able to suggest (in the ENISA paper already mentioned above in paragraph) is a liaison system such as Eisenhower developed in 1943 within SHAEF and which morphed into NATO. In such a system police forces would dispatch trusted officers to formulate pan-European (or preferably global) strategy for dealing with cybercriminals. Their role would be to represent their country's police forces, and within the global strategy they would make tactical commitments to deal with criminals on their own soil and would ask for help with pursuing those who targeted their citizens but were based abroad.

50. We need proper international cooperation—to move beyond the current approach where every national police force targets the same, biggest, multi-national criminal gang and no-one worries about the rest of the top three, let alone the top 10. We must end a situation where cybercrime is a lucrative career choice with a miniscule risk of ever being chased after, let alone caught.

7 September 2011

Written evidence submitted by IET, The Royal Academy of Engineering and BCS, the Chartered Institute for IT (Malware 11)

Please find attached a response to the House of Commons Science and Technology Select Committee inquiry on Malware and Cyber Crime. This response represents the views of BCS, The Chartered Institute for IT, the Institution of Engineering and Technology (IET) and the Royal Academy of Engineering.

We note that the Government Cyber Crime Strategy will be published later this month. We would be willing to comment on this strategy once published, as a supplement to the response attached.

Inquiry Questions

1. *What proportion of cyber-crime is associated with malware?*

We believe that a definitive answer cannot be given. The true extent of the cyber-crime problem goes unreported and unrecorded. Authoritative data has yet to be collected and collated from responsible bodies such as the Serious Organised Crime Agency (SOCA) and the Police National E-Crime Unit. We are cautious

[18] https://www.botfrei.de/en/index.html

about recommending "industry" figures as we believe that in many cases the figures are debatable and in some instance self-serving.

Even with a precise definition of cyber crime or of malware, security researchers cannot do more than guess at statistics by extrapolating from tiny populations. In May 2010, it was generally accepted in the anti-malware research community that there were around 43 million known malicious programs (evidenced by several presentations at the Computer Anti-virus Researcher's Organisation (CARO) workshop in Helsinki). ESET (an antivirus company) claims that as many as 200,000 unique samples of malware can be seen per day. It is hard to be specific however, due to the fact that estimates vary widely from company to company.

It is generally argued that malware is used either directly or indirectly in a significant proportion of cyber crime. A very high proportion of cyber crime has some sort of connection with malware, with most crime being fuelled by botnets (spam, phishing, malware distribution, *Distributed Denial of Service* (DDoS), fake antivirus (AV), captcha breaking, click fraud etc). Malware can be utilised in various and different forms. It can range in complexity from a simple open proxy to an advertisement delivery platform, to something quite advanced such as a self-propagating malware delivery system. Malware has increased in complexity, sophistication and volume, making it more difficult to quantify.

The banks and law enforcement agencies are best placed to provide a more definitive answer on what proportion of cyber crime is associated with malware. Bank customers are asked to report instances of cyber crime to their bank rather than directly to the police; however the banks are said to have an incentive to treat many reports as the fault of their customer and not as crime. Police figures are therefore likely to be lower than the real numbers.

We would like to point out that there is likely to be a substantial increase in cyber crime as more financial transactions are carried out on mobile phones, which are much more vulnerable and virtually unprotected from malware.

2. *Where does the malware come from? Who is creating it and why?*

The usual intention of a malware user is to compromise and potentially control as many systems as possible. Usually malware is created by intelligent individuals who desire either financial advantage, fame or power—power gained from control or the fame gained from being an international cyber criminal. A significant proportion of malware is said to come via emails, mainly through attachments.

The usual sources include organised crime, hackers, and activists; reasons include status, disruption, dissidents, military, business espionage, theft, financial gain and global terrorism.

There are six notable groups associated with the use of malware:

(i) ***"Script kiddies"*** exploit code developed by others and pretend that they are hackers. They are sually only able to attack very weakly secured systems.

(ii) ***Criminals***—Criminals work individually or within increasingly professional organisations and are responsible for credit card fraud and other theft activities. In economically challenged countries with high unemployment, graduates are tending to join these groups. In Russia, there are various groups using a notorious Internet Service Provider (ISP) which has been reported to host websites for illegal businesses. They use professional teams for their criminal objectives.

(iii) ***Hacker groups***—These groups usually work anonymously and develop tools for hacking. They may hack computers for no criminal reason, often to just show their presence. Hacking can also provide a route to employment, with companies often hiring hackers to test their security.

(iv) ***Insiders***—Although they represent only 20% of the threat, they produce 80% of the damage to the systems. These attackers are considered to be the most dangerous group. It is very difficult to identify them as they reside inside an organisation, working as authorised users. Their motives may be criminal or personal.

(v) ***Political/religious/commercial groups***—These groups are not usually interested in financial gain. Governments can deploy considerable resources and technical expertise to develop malware for political ends. The Stuxnet worm for instance, which attacked Iran's nuclear enrichment facilities, was believed to be developed by a foreign government. Malware is said to be also used by commercial companies with the intention of stealing the IPR from their competitors.

(vi) ***Advanced Persistent Threat (APT)/nation state***—This term has been used for some time in government and military domains to describe targeted cyber attacks carried out by highly organised state-sponsored groups, with deep technical skills and computing resources.

Regional variations

Regional variations have been observed in the use of malware. African malware use tends to involve non-technical fraud. Russia and Latin/South America tend to be associated with malware relating to banking/financial fraud and phishing. Russia and Eastern Europe have highly organised gangs devoted to a whole economic framework related to cyber crime, from money laundering to credit card credentials to malware distribution.

3. *What level of resources is associated with combating malware?*

We believe that considerable resources are needed to combat malware. Malware prevention is thought to be a significant expense and drain on resources. Ensuring that all AV, (Anti Virus) signatures are up-to-date is often a full time job for an individual or team depending on the size of the organisation that is being served. It is reported that the United States federal agencies spend about $100 million a year on combating cyber crime through the *Federal Bureau of Investigation* (FBI), Secret Service, National Cyber-Forensics & Training Alliance (NCFTA), Department of Homeland Security (DHS). Large web services firms like Google and Microsoft are thought to spend in the order of $100 million a year each on cyber crime prevention, with smaller firms like PayPal and Yahoo spending in the tens of millions.

We believe that it is impossible to provide a complete defence against malware. It is only possible to provide an effective defence for known vulnerabilities for which that the vendor has supplied a security patch. AV software is only partially effective in detecting malware on a data channel that the software is monitoring. There is no defence against malware that is exploiting vulnerabilities that are only known to the attacker (or malware writer). This means that even with vast resources, an organisation cannot guarantee 100% effectiveness in the detection and elimination of malware attacks.

We have identified five distinct resource types:

(i) **Development resources** are used to design and implement security in a system as it is being built.

On 15 January 2002, Bill Gates, the chairman of Microsoft, informed all employees that security was a top priority, changing the company's strategy. It took Microsoft until 25 August 2004 to make its PC operating system secure, when it released Service Pack 2 for Windows XP. The first PC operating system that was built with security in mind was not until 30 January 2007 when Windows Vista was released, some five years after the company's strategy was changed. Microsoft released Windows 7 on 22 October 2009 which made significant improvements in the security of the product over previous versions. However, there are still vulnerabilities in Windows 7.

Microsoft is the exception. Most vendors of software tend not to incorporate security into their products, as they see the cost as an overhead, with no commercial advantage to them. For example, Adobe found its products targeted in 2010–11, particularly Adobe Reader and Flash, which forced them to have to release out-of-cycle security to address vulnerabilities that were actively being exploited.

(ii) **Research resources** are the resource required to find and identify the vulnerability in a system, whether it is being actively exploited at present or not.

Responsible researchers who have identified vulnerabilities in a system inform the vendor, and allow the vendor time to fix the vulnerability. Malware writers do not inform the vendor of the vulnerabilities they are exploiting. Malware that is exploiting an unknown vulnerability has to be reversed-engineered, which is a highly skilled job and resource intensive.

To fully analyse a specific piece of malware may take weeks or months depending on its level of sophistication. For example, the Stuxnet worm is still being analysed six months after the original detection.

(iii) **Vendor resources** (which also apply to systems developed internally) are those resources required to develop and test a security patch to help with the detection of vulnerabilities.

Vendors who become aware of security vulnerabilities in their products have to develop a security patch that will prevent the malware exploiting that particular vulnerability. However, the vendor has to ensure that the patch does not break any of the existing functionality of the system. The vendor may have to divert resource away from developing new products to developing and testing a patch for the vulnerability.

(iv) **Individual resources** are those employed by an individual to maintain their own system in a good state to defend against malware.

The resources that individuals have to deploy require some technical knowledge. Security patches have to be deployed in a timely manner, and many people simply do not understand the importance of doing so. AV has to be installed, which will then update with the latest AV signatures. We would welcome any initiatives that would help to educate users about the dangers of opening suspicious emails, for instance, the risks associated with opening attachments without scanning them first.

(v) **Organisation resources** are the resources of organisations (government department/agency, commercial organisation, or charitable organisations) used to maintain their systems in a good state in order to effectively defend against malware attacks.

The costs are significant as security patches must be tested before they are deployed. If there is inadequate testing, then the system may no longer work after the patch has been deployed. If the testing takes too long, then the system can become infected with malware before the patch is deployed. To perform effective testing requires that test scripts are developed that enable automated testing to be performed. While the test system does not need to be identical to the live system, it does need to be a realistic representation of the live system to enable valid tests to be performed.

This requires significant outlay in resources to develop the test scripts, and to have the infrastructure in place for the test systems.

While a large organisation can afford to invest in systems, scripts and resources to carry out testing and analyse the test results, this is not realistic for individuals, who must rely on the testing performed by the vendor. Individuals do not have the expertise to monitor for suspicious activity, although this would improve with the provision of educational initiatives, as mentioned in section iv.

4. *What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?*

There are no authoritative statistics. The proportion of infected PCs is variously estimated to be in the 1–15% range; 5% might be a conservative estimate. It has been reported that hostile cyber attacks on companies accounted for nearly one third of all UK data breaches in 2010—up from around 22% the year before, with incidents becoming increasingly expensive.

A survey by the Ponemon Institute found that the cost of a data breach rose in 2010 for the third year running. The average data breach incident cost UK organisations £1.9 million or £71 per record, an increase of 13% on 2009, and 18% on 2008. The incident size ranged from 6,900 to 72,000 records, with the cost of each breach varying from £36,000 to £6.2 million. The most expensive incident increased by £2.3 million compared to 2009.

Impact to individuals

The impact to the individual from a successful malware infection is varied, but can be very significant. Examples include:

(i) The PC becomes part of a Botnet (maybe thousands or tens of thousands of individual computers), which is then used by criminals to distribute Spam email to others, or to launch a denial of service attack against an organisation. Botnets are increasingly rented out for criminal purposes. The owner of the PC may only suffer a loss in performance of their PC, or they may be accused of committing a criminal offence.

(ii) The malware may be used to extract useful information that may be stored on the PC, which could include personal details, bank details etc. For example, the government outlined in December 2010 that it had been a victim of the Zeus malware, with undisclosed loss of sensitive information. The loss of information can have serious consequences for the individual concerned, not only financial loss, but could affect their relationships with others or cause the loss of irreplaceable records such as personal photographs.

(iii) The PC may be used to host illegal content. For example, child pornography. The owner of the PC is then open to being accused of knowingly hosting the illegal content.

The cost of malware infection is very high. Whilst there are some solutions, they tend to be part of a portfolio, which can be expensive. The cost to individual PC users is reported to be in the tens of pounds/ dollars and euros per year in terms of AV expenditure. Furthermore, it is claimed that up to two million people or 4% of the English population are said to become victims of fraud each year. Cleaning up infected corporate networks may cost tens of millions of pounds and take a team of people several months.

Industry effectiveness

By and large, industry is not effective in defending against malware attacks. Many vendors still do not take security seriously. What we are seeing is an arms race, with the malware writers always being one step ahead of the defenders. To quote from a Virus Bulletin article (1 Feb, 2011):

> *"In the mid 90s we were in a position where we could accurately count the number of viruses that had been seen. This was possible for several reasons:*
>
> *(i) The number of new viruses was small enough for each sample to be identified and analysed in detail.*
>
> *(ii) It was easy to determine which part was virus and which part was the infected application.*
>
> *(iii) The size and complexity of the malware was quite limited."*

In 2011, the situation is completely different, with a large variety of malware out on the internet (new variants of a particular malware are produced every day or so). Malware threats have increased in complexity.

AV software vendors have varying degrees of effectiveness at detecting known malware threats. Some large vendors have effectively stopped developing their product five years ago, so may only be 50% effective at detecting known malware.

5. *Should the Government have a responsibility to deal with the spread of malware in a similar way to human disease?*

All malware is in breach of the Computer Misuse Act 1990 and therefore a criminal activity. Malware therefore needs to be viewed in the same way as any other criminal offences. Human disease, in contrast, is natural and may be unavoidable. This is not the case for malware and as such the Government needs to be instrumental in tracing those responsible and prosecuting them accordingly. The biological analogies (virus, worm) should not be stretched to imply that similar control mechanisms would be effective in the cyber domain.

According to the Cabinet Office—see http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime.

> *"The Cost of Cyber Crime" report reveals that whilst government and the citizen are affected by rising levels of cyber crime, at an estimated £2.2 billion and £3.1 billion cost respectively, business bears the lion's share of the cost. The report indicates that, at a total estimated cost of £21 billion, over three-quarters of the economic impact of cyber crime in the UK is felt by business. In all probability, and in line with worst-case scenarios, the real impact of cyber crime is likely to be much greater.*

We therefore believe that the Government should help tackle the spread of malware, to reduce the impact on the UK economy.

We also believe that the Government needs to provide incentives to businesses to protect individuals against such losses. At present, it is not considered a commercial imperative among many organisations.

The Government should consider the following when developing a cyber crime strategy:

(i) **Education**—The website http://www.getsafeonline.org/ provides good advice on security. We would encourage the Government to increase the level of advice it provides to the public about security, in order that people do not remain ignorant about the issues of information security. Users need to be educated in information security to ensure that they are able to effectively protect themselves. The best security systems can be defeated by a user who wilfully and ignorantly overrides them (eg when they are the target of Phishing and Spear Phishing attacks, which dupe people into entering personal data into fake websites). We would again argue that more resources should be given over to explaining the basic security facts and the importance to individuals and industry. Basic lessons in the safe use of computers should be provided regularly to schoolchildren throughout their schooling, starting in primary school, in view of the reducing age at which children become active and vulnerable users of computers and mobile devices.

(ii) **Government contracts**—It is important that the UK Government leads by example. The Government could consider deploying products where the vendor of the product has actively designed security into the product. As in the case of Microsoft, this is not a simple tick-in-a-box exercise, but requires considerable effort to achieve properly. Security has to be designed into the product from the start, and cannot be added on at a later date.

The Government is a large buyer of ICT systems. Consequently, it can have an impact on the marketplace. The Government could have significant influence if a list of more secure products was published. This could result in increased security provision by individuals and organisations, who look to the Government to provide advice.

Furthermore, the Government needs to ensure that its contracts ensure that its own systems are maintained in a secure state. Contracts need to outline which systems should be patched (all should be patched, in our view) and the frequency of patch deployment.

(iii) **Legislation**—Criminals operate in many different jurisdictions, making it difficult to prosecute them.

There are very few convictions under current legislation. Developing malware, and installing malware onto computers, are offences which should be punished with penalties proportionate to the losses caused.

Legislation would also need to make it clear that researchers and vulnerability and penetration testers, who have a contract in place to perform such testing, are not committing an offence.

(iv) **International relationships**—The UK Government needs to encourage other countries to establish appropriate legislation that enables the successful prosecution of criminals who are committing cyber crime. Sanctions also need to be imposed on countries that are harbouring cyber criminals.

There needs to be cooperation between countries on cyber crime. While for some serious crimes such as child pornography, there is cooperation, there is not the same level of cooperation for less serious offences. The cost to the UK economy is estimated at £21 billion a year by the Cabinet Office (see above), with the majority of criminals based outside the UK. The UK cannot solve this problem on its own. It needs the cooperation of other countries to eliminate the threat.

6. *How effective is the Government in co-ordinating a response to cyber-crime that uses malware?*

We are unclear on the detail of the Government's strategy toward cyber crime associated with malware. We do, however, strongly believe that it is the responsibility of the government to try and prevent cyber crime.

We would like to see renewed focus by the Government in preventing exploitation of its core departments by its competitors overseas and lead by example. We would also argue that the police need to be better resourced to combat cyber crime, and to ensure that all criminal malware use is prosecuted. This will need to be done in conjunction with any educational initiatives that ensure individuals and organisations are aware of malware threats and the importance of security provision.

7 September 2011

Written evidence submitted by the Serious Organised Crime Agency (Malware 13)

Introduction

1. This submission sets out the Serious Organised Crime Agency's (SOCA) written evidence to the Science and Technology Select Committee's inquiry into malware and cyber-crime.

2. SOCA works with its partners, under the UK Control Strategy for Organised Crime, to address the threat of organised cyber crime, which it defines as:

- Offences in which computers, networks or the data held within them are specifically targeted by an Organised Crime Group (OCG) including the design, sale or use of tools and techniques needed to mount such attacks, and the use of virtual payment systems to launder the proceeds of crime.
- The use of ICT by OCGs to enhance operational security or effectiveness which includes alternative communication methods and evidence denial.

Malware is an umbrella term for malicious software and it is therefore used to describe any piece of software that is designed for a malicious purpose. As such, malware describes the collection of tools that can be used by individuals for a malicious or criminal purpose. It is not one single group or type of software that executes one particular type of crime. SOCA's operational focus, where malware is concerned, is on the individuals behind the creation and deployment of those systems which represent the biggest threat to the UK.

3. The submission outlines the current level of knowledge within the organisation on malware and cyber-crime. This submission has been written in coordination with the Home Office, and should be considered supplementary to its submission which addresses the full range of questions the inquiry is set to explore.

What proportion of cyber-crime is associated with malware?

4. Malware is a key enabler of internet-enabled fraud. Cyber criminals use the internet as an opportunity to gather personal information or data, with the aim of exploiting it for financial gain. SOCA sees a continuous development of methodology as both criminals and those opposing them react and counter-react to an ever changing landscape. Developments in both technology and public take-up have meant that the tactics used by cyber criminals evolve at a rapid rate. The use of malware within cyber crime has also risen in conjunction with improved public awareness of scams such as phishing.[19]

5. A significant proportion of cyber-crime uses malware to perform some part of the crime. Even spamming[20] now involves the use of malware, as the majority of spam messages are now delivered using Botnets.[21] Criminality has had to evolve and develop increasingly sophisticated ways of capturing data and that increasingly means the use of malware, in one form or another. The UK is a relatively developed market for internet use and so the awareness of simple spam emails is perhaps greater than in countries where the internet is new. For this reason, criminals need to employ increasingly more sophisticated methods to achieve their aims as the user's defence becomes similarly more sophisticated.

Where does the malware come from? Who is creating it and why?

6. Historically, malware was created by small numbers of people who had the necessary technical skills. Deployment of malware (and the consequent profit to be made) was similarly restricted to a small number of individuals. However, as cyber-crime has evolved, a complex marketplace has developed, allowing specialists (such as malware writers) to sell their products to others with little or no technical ability.

7. Organised crime groups have been known to commission malware creators to produce the tools they require, and malware writers have also been known to produce "off-the-shelf" items; an example being the Zeus financial malware that was openly available for purchase for approximately US$700. In addition to the market for generic malware families (eg Zeus, SpyEye, Gozi etc) a new market has emerged for bespoke attack modules targeting specific financial institutions / corporate victims. This means that relatively dated malware families can still employ state-of-the-art attack tools, maintaining their effectiveness. Malware (such as Zeus) is also available with technical support, including a 24-hour telephone helpline. Criminal fora where such

[19] Phishing is when an individual receives an unsolicited email purporting to be from their financial services provider, asking for "account verification"—usually including a link to a fake website—from which criminals will harvest the financial data for fraudulent activity.

[20] Spam: Using electronic messaging systems to send unsolicited bulk messages indiscriminately.

[21] A Botnet is a collection of compromised computers connected to the Internet, termed Bots that are used for malicious purposes and controlled by a single source.

transactions are made have been in existence for at least a decade. These fora are frequently hosted in jurisdictions where UK Law Enforcement have little influence, and have stringent membership policies.

8. The main geographical source for the creation of malware targeting UK financial institutions is Eastern Europe, from former Soviet States. The socio-political conditions in some of these countries are ideal: education and internet development is reasonably good, employment and salary potential low, law enforcement deterrent is not prohibitive and organised crime groups exist. Past emphases on scientific or technical education has led to a highly able workforce with few legitimate prospects that can equal the criminal market in terms of financial reward.

9. This financial reward is the main driver behind malware creation. The early days of cyber-crime saw criminals developing attacks for kudos and peer recognition. This has dissipated and now status only accounts for a small amount of the activity for which SOCA has the remit to investigate. State-sponsored threats and "hacktivism" (both significant sources of new malware) fall outside the scope of SOCA's focus, but information is shared with its UK partners where necessary.

What level of resources is associated with combating malware?

10. In April 2011 as part of the Strategic Defence and Security Review (SDSR) outcomes, SOCA was allocated £19 million over four years to support the delivery of a wider National Cyber Security Programme (NCSP).[22] SOCA will use this funding to support the Government's priorities on cyber crime in the following ways:

— by increasing the capability and capacity to collect, analyse and disseminate intelligence on cyber-crime and cyber criminals;

— by providing an effective criminal justice response to cyber-crime through the enhancement of capabilities and the delivery of high-end operational outcomes. It will also provide additional legal services to deliver expert tactical and strategic support;

— by working with law enforcement, intelligence agency, private sector and academic partners to maximise use of technical and other capabilities for the benefit of all parties;

— by focusing dedicated resource to the delivery of high volume interventions to disrupt criminal cyber activity;

— by increasing private sector and public awareness through enhanced dissemination of timely intelligence and warnings via diverse media channels and Alerts; and

— by establishing a dedicated overseas resource to tackle cyber criminality in partnership with local law enforcement and other agencies and provide additional legal services to deliver expert tactical and strategic support to enhance international law and improve international co-operation.

11. Significant successes achieved against cyber crime in recent years include:

— Working with GetSafeOnline.org, SOCA identified a highly organised criminal operation employing "scareware" to trick web users into revealing their financial information to cybercriminals. Potential victims received messages on screen or a call from an IT "help centre" claiming that their computer might be infected by a virus or other malicious software. A fake scan of their computer was then used to convince the victims that they needed to download new security software. In reality, victims were paying cybercriminals for the privilege of installing useless or malicious software onto their computer. Get Safe Online adopted this threat as the main theme for their 2010 campaign and SOCA provided advice to members of the public on how to spot "scareware" and how to avoid becoming victims of this type of crime;

— SOCA is systematically targeting the criminal trade in stolen financial information. In 2010–11, SOCA seized 1.4 million items of compromised payment card data from cybercriminals and passed these details to UK Payments via its Alerts system. This data has subsequently been used to prevent fraud and identify theft where security breaches have occurred. The success of this approach has encouraged law enforcement colleagues in the US, Europe and Australia to participate in the initiative;

— Following a SOCA investigation, Virgin Media earlier this year wrote to about 1500 customers to inform them of a compromise. This was the first time that SOCA has partnered with an ISP to proactively contact its customers and is seen as a positive step in the corporate / law enforcement partnership; and

[22] Led by the Office of Cyber Security and Information Assurance (OCSIA) in the Cabinet Office.

— SOCA led the UK end of a long-term FBI undercover operation against the online criminal forum DarkMarket. Before the forum was closed down in October 2008, it had been regarded as one of the most significant internet sites dedicated to the theft and sale of compromised personal information. It dealt in large quantities of stolen payment card and online banking data, and the tools and techniques needed for criminals to commit offences using them. Alongside two SOCA operations against DarkMarket subjects, SOCA provided intelligence and forensic support in this work to the City of London, Greater Manchester, South Yorkshire and Humberside Police. Follow up work continued, with suspects arrested in Turkey, Germany, the US and the UK, of whom 12 were arrested here.

12. Going forward, the National Crime Agency (NCA) offers an outstanding opportunity to achieve a further step change in the response to organised crime, including through more effective national tasking and coordination arrangements. The NCA also 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 national centre of excellence on cyber crime which it will host.

What is the cost of malware to individuals and how effective is the industry in providing protection to computer users?

13. At a superficial level, individual citizens may feel little direct financial impact from malware. Financial institutions will often cover the cost of a loss. It is assumed that these costs are covered by higher charges elsewhere, but the detail of this is not known to SOCA. Crime such as identity theft may not result in a financial cost but it could have a traumatic effect nevertheless.

14. General information on the financial impact of malware is inconsistent. At a corporate level for example, a large financial institution may not wish to disclose malware costs for fear of reputation damage. There is a better understanding of the threat in the US due to mandatory requirements to report data breaches in most US states. In the UK there is no obligation to disclose, and estimates of the costs of malware are difficult to assess.

15. Trade on and use of the internet has grown. In the future, it is likely that every age group will use the internet extensively. Attitudes to sharing personal data online have already undergone a marked change. Confidence in using the internet is therefore important and malware undermines that confidence, resulting in opportunity cost. Industry measures to protect their customers vary, and SOCA is committed to working closely with companies to mitigate the threat posed.

7 September 2011

Written evidence submitted by the Police Central e-Crime Unit (Malware 14)

Introduction

1. This report complements the Home Office submission to the Science & Technology Committee.

2. This Police Central e-Crime Unit submission addresses matters 1–3 as outlined in the Science & Technology Committee's Terms of Reference for Malware and Cyber crime.

3. For operational reasons the nature of the evidence provided has been restricted to a limited number of completed cases.

4. For the purposes of this submission, the Home Office "United Kingdom Threat Assessment of Organised Crime" definition of malware has been adopted: Malicious software consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorised access to system resources, and other abusive behaviour.

1. *What proportion of cyber crime is associated with malware?*

Remit of Police Central e-Crime Unit

5. The MPS's Police Central e-Crime Unit (PCeU) is the national lead for e-Crime. The PCeU remit is to tackle those responsible for the most serious incidents of:

— Computer intrusion;

— Distribution of malicious code;

— Denial of service (DDoS) attack; and

— Internet-enabled fraud.

6. The PCeU proactively targets individuals involved in the high level authoring, distribution and criminal use of malware. These individuals are key enablers for cybercrime causing substantial harm to the UK and global economy.

7. Just over half (55%) of PCeU's current investigations involve the authoring, distribution or utilisation of malware.

8. In the context of PCeU investigations, malware is primarily utilised in the commission of fraud offences against the financial sector.

9. A recent and growing area of concern for law enforcement is the use of Distributed Denial of Service (DDoS) attacks against organisations in the wake of the wikileaks scandal. For the purposes of this submission, only the criminal use of Low Orbit Ion Cannon DDoS utility[23] is included.

2. *Where does the malware come from? Who is creating it and why?*

10. Malicious software is predominantly created, distributed and used for financial gain and DDoS attacks.

Attacks Against the Banking Sector

11. Organised Criminal Groups (OCGs) utilise malware to attack the banking sector. This form of e-crime can be extremely profitable, over a relatively short period of time, when compared to more traditional crime types.

12. Financial institutions invest heavily in Information Assurance. Criminals attack banking systems through the most vulnerable point, the on-line banking user.

13. OCGs investigated by PCeU are primarily using Trojan malware, typically SpyEye and Zeus, to create Botnets which are controlled by a server which can access bank accounts and transfer money out.

14. Malware infects victims' personal computers, waits for them to log onto a list of specifically targeted banks and financial institutions and then steals their personal credentials, forwarding the data to a server controlled by criminals. It can also manipulate web browsing sessions including creating an additional page requesting the victim to reveal more personal information, such as payment card number, PIN, and passwords. Users have no idea they are being defrauded.

15. Unbeknown to the owner, computers infected with Zeus or SpyEye become part of a network where they fall under the remote control of computer criminals.

16. PCeU operational findings reveal that OCGs demonstrate a highly systematic approach to this form of criminality. Investigations have highlighted the use of technical expertise by OCGs in the form of malware authors, who provide the essential IT support for this criminality.

17. PCeU's Virtual Task Force (VTF) approach has gone some way to mitigate against the risk of successful large scale attacks against the financial sector in the future through encouraging intelligence sharing.

DDoS Attacks

18. While the threat of DDoS attacks can be used to extort money from commercial organisations. The recent cases dealt with by the PCeU have involved the use of DDoS tools to attack organisations based on ideological grounds or simply to prove technical prowess amongst peers.

19. There has been a growing recent trend in "Hacktivism" encountered by the PCeU which has involved groups or individuals targeting the websites of companies and organisations, motivated by political or ideological goals. This has been particularly highlighted by recent activity around Wikileaks supporters such as "Anonymous". This has demonstrated that, facilitated by social networking sites, large numbers of individuals globally are able to voluntarily use their computers to launch DDoS attacks against organisations, with a low degree of central organisation or leadership utilising user friendly software such as LOIC (Low Orbit Ion Cannon DDoS utility).

20. There are individuals who author without affiliation to political groups or desire for money but who are motivated by factors such as the personal challenge of testing their IT skills. These individuals will carry out a range of attacks from DDoS to hacking and defacing websites. These individuals are more akin to the stereotypical lone, male hacker or "script kiddy".

The Authoring and Distribution of Malware

21. PCeU operational intelligence suggests that there are a relatively small number of individuals with the technical skills required to produce the code involved in distribution of malware.

22. Some individuals provide bespoke malware services to OCGs while at the same time working on their own criminality. Lower tier individuals appear to be "testers", checking for bugs in the scripts which are used to move money into mule accounts and making adjustments to the code as required. Identified OCG's have members each using core skills which are distinct ie infrastructure, cash out and code development.

[23] Low Orbit Ion Cannon DDoS utility (LOIC) Originally originally developed for network stress-testing, but later released into the public domain where, years later, it became a weapon of choice for hacktivists. Floods a targeted site with TCP or UDP packets, a relatively unsophisticated yet effective approach, especially when thousands of users use the tool to join voluntary botnets. By default does nothing to hide a user's identity

23. Methods of malware distribution continue to evolve. A recent PCeU operation has shown that malware propagation is moving onto compromised legitimate websites, which may indicate that spam delivery and fake websites are no longer the primary mechanisms. Also this operation has found a number of Command and Control Servers used to both store the stolen data and control the malware. These servers are hosted in Russia, China and the UK.

Online Criminal Forums & Malware "Kits"

24. Online Criminal Forums allow all types of criminals to interact with each other across large geographical areas, to plan, organise and commit crimes, without having to personally know each other. These types of forums enable criminals with different skill sets to advertise their services and thus create virtual OCGs that would not have formed in off-line environments. Disturbingly, they also act as an educational forum to the benefit of new members.

25. PCeU has gathered intelligence and investigated the use of online criminal forums by a range of different individuals and groups including hacktivists, OCGs and individual hackers to share knowledge and organise offences.

26. Online criminal forums facilitate the purchasing of "malware kits" which enable individuals to carry out "ready made" attacks with less technical knowledge or experience. Intelligence gleaned from PCeU investigations indicates that individuals with little prior knowledge of IT can develop the capabilities to carry out a malware attack within a very short period of time.

27. Online criminal forums and "malware kits" regularly come to the attention of PCeU staff investigating banking Trojans and DDoS attacks.

28. Availability via criminal forums, the relative ease of use and sometimes low cost of Zeus and SpyEye malware in particular, has led to its popularity and extensive proliferation globally.

Case Studies—The Authoring and Distribution of Malware

29. A PCeU investigation into an individual who was running a Zeus Botnet, in addition to hosting an online global crime forum called GhostMarket.net. GhostMarket was the largest English speaking criminal forum with over 8,000 members which promoted and facilitated the electronic theft of personal information. In addition to allowing users to trade compromised credit cards, the forum facilitated the creation and exchange of malware, the establishment and maintenance of networks of infected personal computers (Botnets) and the exchange of information about cyber and other criminality. Five individuals were arrested and charged, with all submitting guilty pleas after charging included Intentionally / Encouraging an Offence under the Serious Crime Act 2007. Though loses through criminal activity linked to the forum are still be calculated, the estimated value is currently in excess of £20 million.

30. A PCeU investigation into an OCG utlilising "Drive by Download" methodology. "Drive by Download" is where malware is inserted into a website thus allowing the infection of any computers visiting those domains. This investigation has identified that the subjects have been involved in the compromise of UK and global bank accounts using SpyEye and Zeus for financial gain. Over 100 malicious domains were identified in this investigation.

31. A PCeU investigation into an individual who is administrating a server, hosting both botnets and malicious software. Intelligence suggests that these are being used to commit criminality by stealing financial credentials from UK victims.

Case Studies—Utilisation of Malware

32. PCeU's operations have shown the significant criminal gains that can be achieved through organised, malware-facilitated, banking fraud. Alongside the financial sector Virtual Task Force (VTF) the PCeU dismantled the international OCG utilising a Zeus Trojan.

33. Over a 90 day period, the OCG was able to redirect funds from compromised UK bank accounts to the evidential value of £2.66 million from the 285 accounts. Intelligence suggests that there were significantly more accounts affected and therefore potentially much greater losses. These figures only consider losses to UK banks. The OCG involved was also targeting banks in the USA, other Western European countries and Australia. Total criminal gains may never be calculated. In the USA alone, this OCG stole $70 million.

34. The PCeU arrested three men in April 2011 in connection with an investigation into the use of toolkit SpyEye malware to steal online banking details. The international investigation revolved around the group's use of variations of the SpyEye malware. This malware has the capability to harvest personal banking details from internet users and send the results to remote servers under the control of criminals.

35. More recently, the PCeU investigated a case where Trojan malware was hidden within bogus job advertisements posted on Gumtree. When individuals downloaded the application form for a job their computer was then infected with a virus. The virus being a Trojan, designed to capture the recipients banking details. The PCeU have made two arrests to date.

3. What level of resources are associated with combating malware?

36. The remit of the PCeU set out in paragraph 5 includes combating malware and as such the full resources of the unit are available to those areas of cyber crime.

37. The additional funding of £30 million over four years has provided the scope to significantly increase the number of cyber crime operations that the PCeU can conduct, by increasing their capacity. The principal aim of which is to provide a level of £504 million of harm or potential harm reduction, experienced by UK society through cyber crime.

38. The following paragraphs explain the different teams within the PCeU that collectively provide the national response to tackling cyber crime, including malware attacks.

39. It should be noted that the specific resources and staff numbers deployed within the PCeU have delivered significant success in responding to cyber attacks invlolving malware as the unit has established a unique concept of operations whereby it has the relationships and protocols in place to call upon the wider policing resources and external industry partners to work operationally with the team thereby enhancing the units expertise and resource capability.

Intelligence Development Team

40. The PCeU Intelligence Development Team (IDT) is staffed by one Detective Inspector (DI) two Detective Sergeants (DS), five constables and four police staff.

41. The role of the IDT is to receive and analyse intelligence which the team then develop by working with the source to produce actionable operational products from which a decision is made whether to progress investigations to the unit's Enforcement teams.

42. In a number of cases attacks are aimed at financial institutions and it is the teams' responsibility to act as the point of contact with these organisations. In addition, the team receives tasking requests from both within the MPS and from outside partners. These requests are filtered against the case acceptance criteria for the unit which focuses resources on the most serious cyber crime incidents. There is a process for the prioritisation of tasks, which is undertaken through a formal weekly meeting that determines and then prioritises operations against threats, risks and the capacity of the unit.

The Enforcement Team

43. The PCeU Enforcement Team provides the investigative and arrest capability of the PCeU and is currently staffed by two DI's, four DS's and 20 DC's (Detective Constables). The team is evenly divided into four pods, each headed by a DS. Operations are allocated:

- The PCeU Intelligence Development Team.
- Fast-time, in direct response to an attack on a financial institution.
- In support of national security operations.
- In support of other foreign law enforcement agency investigations (eg FBI).

44. The PCeU currently works with national, European and international partners in order to call upon and coordinate enforcement activity.

45. The PCeU works closely with the IT security industry, utilising partnership relationships where possible to identify malware-related cyber crime and the subsequent reverse engineering to evidence and attribute the criminal nature, culpability and mitigation techniques.

46. Cooperation between European countries with regards to e-crime has improved significantly in the last three years. This is as a result of extensive operational engagement with countries willing to undertake proactive tasking at the behest of other nations. PCeU facilitates joint meetings to discuss cross border issues, ensure de-confliction and post operational sharing of learning and to improve working practices.

The Technical Team

47. The PCeU Technical Team provides the PCeU with the ability to interrogate digital media and technology with an increasing need for live forensic capability to respond to multi-layered technology and techniques used to commit criminality.

48. The team obtains intelligence and evidence of cyber crime, together with the facility to dismantle Botnets and undertake live network investigative functions.

49. Current staffing levels for the Technical Team are one DI, three DS's, seven DC's and four members of police staff.

50. The PCeU Technical Team's current roles and responsibilities are:

- To conduct computer forensic examinations / investigations, data recovery and electronic discovery.
- To gather and disseminate relevant and quality intelligence.

— To provide technical advice and assistance to officers engaged in the investigation.

— To produce evidence in a form which is admissible in court.

— To provide advice to industry and law enforcement colleagues.

51. The Technical Team's expertise is a crucial element to PCeU investigations and in order to maintain their abilities to combat the range of cyber crime methods, ongoing training and the retention of expertise are key to its success.

The Internet Governance Team

52. The Internet Governance Team comprises of one PS (Police Sergeant), one PC (Police Constable) and a member of police staff. A Detective Inspector also has portfolio responsibility for strategic engagement to identify and establish best practise and changes to national and international protocols within law enforcement and industry.

53. The responsibility of the team is to identify and take action against websites which cause harm to the UK economy through fraud, identity/brand theft and the infringement of property rights.

54. The team has forged links with internet governance bodies both domestically and internationally, as much of the illicit activity is committed outside the boundaries of the UK. Through these relationships the team has been able to remove elements of the criminal infrastructure to reduce the ability of criminal networks to cause significant financial loss. For example, by utilising the assistance of IP providers and domain name registrars sites have been taken down swiftly and to long-term effect.

55. The team is in the process of providing a Standard Operating Procedure for the internet governance position to roll out within policing and other UK Law Enforcement Agencies. This will increase policing capability, assist in the dissemination of best practice and help standardise activities.

56. In addition to those teams outlined, the PCeU also incorporates Cyber Industry Liaison, a Strategy, Performance and Communication Unit and supports the National e-Crime Programme through a National Delivery Office to deliver a regional capability with three hubs supported by the PCeU.

September 2011

Written evidence submitted by Nominet UK (Malware 18)

Introduction

1. Nominet is the registry for the .uk country code top-level domain (ccTLD). With over nine million registered domain names, we are the second largest country-code top-level domain. We are a SME with a turnover of around £21 million and employing about 120 people.

Resources Committed to Combating Malware

2. We do not keep separate records of our expenditure to address malware: this is considered as an integral part of our standard operating costs.

3. As an infrastructure company, we size our systems to respond to possible attacks. We operate our DNS systems with an oversized infrastructure in order to respond to threats such as Denial of Service attacks. We share information with other leading actors in the domain name industry to identify threats and development of attack strategies.

4. The domain name industry has a good track record in working together on sharing best practice and information about risks. In addition to ad-hoc cooperation and specialist associations, the main mechanisms for this are:

(a) ICANN (the Internet Corporation for Assigned Names and Numbers, a US-based not-for-profit public-benefit corporation established to help coordinate the Internet's naming system). We are actively involved in the technical coordination work and a senior staff member is on the Security and Stability Advisory Committee; and

(b) CENTR (the European registry managers association with 50 Full Members, 10 Associate Members and 12 organisations granted observer status) brings together a global partnership of registry operators: Full and Associate members of CENTR represent around 80% of total global ccTLD domain name registrations, and VeriSign, PIR and Afilias, which operate .com, .net, .org and .info, are also Associated Members. The organisation provides an excellent framework for sharing information, for highlighting best practice, and for identifying trends and developments.

5. Nominet is also playing a leading role in researching and deploying defences against future threats to the security of the internet. One area of considerable activity over the last eighteen months has been the deployment of DNSSEC (DNS Security Extensions). DNSSEC protects against forged DNS data (for example, from DNS cache poisoning) by providing digitally signed records. We have signed .uk and .co.uk. We work at the forefront

of DNS monitoring and are developing tools that identify threats such as botnet, spam and denial-of-service attacks.

6. We have worked with other organisations to respond to cyber-crime attacks, in particular where this has involved the use of the domain name system to deliver botnet instructions. This was the case with the Conficker worm where there was a major international mobilisation in response to the threat.

7. While we are not a member of a CERT (Computer Emergency Response Team), Nominet does provide a 24/7 CERT-type function and we do cooperate with other leading players in network and information security. We have a dialogue with CPNI and OCSIA which would allow us to be included in any national emergency planning or exercises. We were involved in the last (US-led) Cyber Storm exercise.

8. We have a significant research effort into ways of assessing "bad traffic" on the Internet and, in particular, looking for patterns showing abnormal behaviour. We are currently spending approx £0.5 million annually on such proactive research.

9. In summary, this work is integrated into our business and it is impossible to identify actual malware-related costs. However, the costs are a significant proportion of our total turnover.

Coordination of Efforts

10. As will be seen above, Nominet is well networked with other businesses, government agencies and international organisations. We are a membership organisation and most of the UK's communications infrastructure companies (and all of the largest ones) are Nominet members.

11. This cooperation is important in a sector as rapidly changing as the Internet. The international nature of communications also makes it important to network across borders with trusted interlocutors—hence why we devote considerable effort to working with international partners.

12. Increased government involvement with trusted parties involved in network and information security—in particular in sharing information—would be welcome. Such involvement is best through cooperation and partnership. The speed of innovation, the transnational nature of the Internet and the number of organisations involved in assuring the successful operation of what was designed as a distributed network requires a cooperative, rather than a centrally coordinated, approach. This was recognised in the conclusions of the World Summit on the Information Society in 2005 and led to the implementation by the United Nations of the multi-stakeholder partnership approach of the Internet Governance Forum.

13. One area where the government could help is in promoting the development of a national CERT, providing a framework for improved cooperation. Any such body should have as a key role to develop networks both nationally and internationally.

14. The analogy with human disease is not a helpful one: the government can certainly help address issues by improved education and awareness, but even in this area a multi-channel approach is likely to give better results. As we have discovered in the five years of the Nominet Internet Awards, many organisations are active in working with different community groups.

15. Government funding for academic research will continue to be important. Government can also show the lead in adopting best practice and in being an early adopter for security enhancements. However, the significant role is for the government to work in cooperation and partnership with other key players.

7 September 2011

ISBN 978-0-215-04155-5

9 780215 041555

PEFC
PEFC/16-33-622

Printed in the United Kingdom by The Stationery Office Limited
02/2012 015012 19585