



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

WEDNESDAY, 19 AUGUST 2009

CANBERRA

BY AUTHORITY OF THE HOUSE OF REPRESENTATIVES

INTERNET

Hansard transcripts of public hearings are made available on the internet when authorised by the committee.

The internet address is:

<http://www.aph.gov.au/hansard>

To search the parliamentary database, go to:

<http://parlinfoweb.aph.gov.au>

HOUSE OF REPRESENTATIVES
STANDING COMMITTEE ON COMMUNICATIONS

Wednesday, 19 August 2009

Members: Ms Neal (*Chair*), Mrs Hull (*Deputy Chair*), Mr Billson, Mr Bradbury, Ms Collins, Mr Georganas, Mr Lindsay, Ms Marino, Ms Rea and Ms Rishworth

Members in attendance: Mr Bradbury, Ms Collins, Mrs Hull, Ms Marino, Ms Neal and Ms Rea

Terms of reference for the inquiry:

To inquire into and report on:

The incidence of cyber-crime on consumers.

- a) Nature and prevalence of e-security risks including financial fraud and theft of personal information:
 - Including the impact of malicious software such as viruses and Trojans.
- b) Implications of these risks on the wider economy:
 - Including the growing economic and security impact of botnets.
- c) Level of understanding and awareness of e-security risks within the Australian community.
- d) Measures currently deployed to mitigate e-security risks faced by Australian consumers:
 - Education initiatives
 - Legislative and regulatory initiatives
 - Cross-portfolio and inter-jurisdictional coordination
 - International co-operation.
- e) Future initiatives that will further mitigate the e-security risks to Australian internet users.
- f) Emerging technologies to combat these risks.

WITNESSES

PUTT, Dr Judy, General Manager, Research, Australian Institute of Criminology 1

SMITH, Dr Russell G, Principal Criminologist, Australian Institute of Criminology 1

Committee met at 12.41 pm**PUTT, Dr Judy, General Manager, Research, Australian Institute of Criminology****SMITH, Dr Russell G, Principal Criminologist, Australian Institute of Criminology**

CHAIR (Ms Neal)—Thank you very much for joining us for this public hearing. It is very much appreciated. I realise your time is probably in high demand. You are very welcome. Although the committee does not require you to give evidence under oath, I should advise you that this hearing is a legal proceeding of the parliament and warrants the same respect as proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as a contempt of the parliament. You will be provided with the transcript shortly after the hearing. If there are any errors in that, could you let the committee know as soon as it is convenient for you. Please make an introductory statement, if you so desire, and then we will open up to questions from the committee.

Dr Smith—Thank you for inviting the Australian Institute of Criminology along today. I am the program manager for the area of research that looks at global economic and electronic crime, one of the research sections at the institute.

Dr Putt—I am a last-minute ring-in. Dr Choo was going to be here as a witness. He is an expert in this field. Unfortunately, he is unwell today. I am here really to provide more generalist support.

Dr Smith—Dr Putt has agreed to provide some brief background information about the work that the institute does, so we will start with the slideshow that deals with that. I will hand over to her.

A PowerPoint presentation was then given—

Dr Putt—The Australian Institute of Criminology is a statutory authority. We were established in 1973. We are primarily funded through direct appropriation from the federal government. We have legislation that defines our mandate, which is to do policy and practice relevant research. We are a relatively small organisation. At the moment we have about 60 people, of whom about 40 are researchers. Having said that, I think we cover the field quite well in terms of the range of crime and justice issues that we research. One of the areas where we have been building up our expertise over the years has been cybercrime. In particular, Dr Smith has led the charge in drawing people's attention to this type of crime from its early stages to when it became quite visible in the public domain, and has continued to do research in this field. We got some funding some years ago from the Australian Federal Police to do research on high-tech crime. That produced a range of material which is in the public domain and is referenced at the end of our submission to the committee. I will not say anything more about the institute. The slide draws your attention to who our current director is and the fact that we have a board of management with state, territory and federal government representatives on it.

Dr Smith—We have circulated a printed copy of the submission which we sent in some time ago and a copy of the PowerPoint slides, which I would like to go through briefly now. I might start by mentioning the types of research that we have done. I am aware that the committee is

looking principally at the risks for consumers—individuals—as opposed to the cybercrime risks that might face businesses and government departments, but of course there is some overlap in the areas we have been looking at. They fall into three broad areas. There is financial crime and principally the area of personal fraud and scams, which are synonyms really. Those terms get used variably. The Australian Bureau of Statistics has adopted the term ‘personal fraud’ but it really just means scams—invitations to respond to requests that come mainly by email.

We have also done a lot of work on identity related crime. The current term of art there is ‘identity crime’, which encompasses identity fraud, where funds are sought to be derived in various ways; and identity theft, in which people make use of another living or deceased person’s actual identity to perpetrate a fraud.

We have done further research into risks facing electronic banking—that is, the risks of illegal transfer of funds between accounts, and a range of business fraud opportunities. The linking theme behind all of those is some misuse of identity information, either individual or business. There are a number of cases of people setting up businesses using false identity information and then using that business entity as part of the means of extracting funds.

In terms of the public sector, we did some research a number of years ago that looked at risks for government in the areas of electronic voting, misuse of electronic taxation—online tax with the Australian Taxation Office—and abuse of that part of Medicare that operates electronically. Again, those types of crimes are often linked by misuse of identity. Sometimes there might be criminals who have set up fictitious identities as medical practitioners in order to claim funds from the government.

In the area of personal cybercrime, a number of years ago we looked at intellectual property crime, and of course a lot of that now takes place via the internet—for example, people downloading movies without authorisation. It is now extending into the corporate world, with intellectual property that businesses hold being obtained illegally by people hacking into business networks and computers and making extortion attempts.

Recently my colleague Dr Choo, who is not here, did some research on online child grooming and cyberstalking. Essentially, the same sorts of activities that take place in the terrestrial world are now being committed using email and chat rooms.

Finally, there has been some research on internet gambling. That is really just looking at the ways in which online gambling businesses can be manipulated for financial gain.

The slide I have here I present for two reasons. One is to give you an idea of the range of types of cybercrime that exist and have existed over the years. You can see that they start from the early misuse of telecommunications systems. The first we were able to find dated back to 1867, when a telex service between the east and west coasts of America was intercepted by some individuals who manipulated the share market by putting false information into that telex communication—so a very early case of cybercrime before we even had computers, but it is essentially using the same strategy.

Then we have a number of types of illegality involving telephones, fixed-line telephone services, in the sixties and seventies: people manipulating billing systems on telephones to get

access to free phone calls, which is known as phreaking; and telemarketing—people setting up operations to trick people into engaging services to gain money. From the late seventies, when we started seeing computers being used more widely, we started having risks of people gaining access to networks improperly, which is known as hacking. It has been called cracking, if there is an illegal, nefarious motive behind the activity, although it is popularly known as hacking. Then we had the risks of viruses when email started to be used more widely, and there were denial of service attacks and other forms of financially related fraud.

So the purpose of this slide was really to show that a lot of the risks have been around for a long time and the development in cybercrime has really followed the development of technology. As new technologies have been created—telephones, the internet and wireless systems—they have all been targeted. But the underlying motivations are fairly constant.

This next slide looks at the changes in motivations. When cybercrime first became a problem in the early eighties, a lot of the computer so-called geeks who were involved in this often did so out of reasons of curiosity or to test their skills against the security industry. So it was not so much a financially motivated problem but more of a challenge for often a clever young person. Particularly in the very early years, a lot of the cybercriminals were quite young computer geeks. A famous case in the seventies involved Captain Crunch, who you might have read about, who was able to manipulate a billing system and telephone by using a toy whistle—which, when you blew into the telephone handset, disabled the billing system of the telephone network and let you make free calls.

Mrs HULL—By using a whistle?

Dr Smith—That was discovered accidentally but it became popular. In the eighties, people started to see that there was a lot of kudos attached to being a successful cybercriminal, and people like Kevin Mitnick in the United States sought out very high-profile targets—departments of defence, banks and other high-profile government agencies—just to gain access to their networks to alter material, not so much to cause damage but to make their presence felt. It might be called fame-seeking. Following that, there were some types of cybercrime that were essentially personal types of crime—with personal motivations. You can see things like cyberstalking, dissemination of obscene or racist materials and computer vandalism—people taking revenge against other people or businesses to make some point—but they were largely motivated by personal reasons.

The main change which took place in the 1990s and is facing us at the moment is the problem of financially motivated offenders. Cybercriminals now tend to be people who are organised, sometimes in quite sophisticated groups where individual specialists in different parts of the fraudulent strategy will group together. Some people will do one part of the scam that they are skilled in and another person will do another part. That requires some coordination. That would largely be to gain money and can be disguised in various ways through counterfeiting websites, through phishing attacks, through to the other types of businesses out there which are manipulated. A lot of the pornography websites are really just fronts for getting people to disclose personal information. They are not so much interested in the content; it is really to get access to people's bank account information.

Finally, there has been considerable discussion over the last decade so about the risks of politically and ideologically motivated offenders, particularly terrorist groups who might wish to attack the infrastructure of governments in countries. Although the risks are there, there is not a great deal of documented evidence of incidents actually taking place, although there are some very likely scenarios that we need to be careful of. One example I would like to mention in passing is an incident which was motivated by revenge in Queensland in which an offender gained access to a sewage treatment plant and changed the settings on the system, enabling sewage to be dispensed into the countryside as an act of vandalism. That is the risk of someone gaining access to a national infrastructure which could be used by politically motivated individuals.

Ms NEAL—The scenario of many fictions in that regard is the computer-controlled missile attack. I do not think I have heard of it in real life but many films seem to have the scenario where terrorists gain control of missiles and shoot them off randomly, or not randomly.

Dr Smith—Unfortunately, all military infrastructure is electronic in recent times and that creates the same risks for things like banking. If banking systems can be manipulated, then departments of defence can be as well. The risks are certainly present.

Mrs HULL—Concerning cyberstalking and pornography, have you seen a rise in young people being targeted through mobile phones?

Dr Putt—Edith Cowan University released some research in the last few months which is trying to look at the extent of the problem. We are at the stage of trying to map how widespread it is, rather than being in a position to comment on trends over time. That is the first large scale study I have seen looking at how many young people report they have been exposed to some form of stalking or other kinds of abusive behaviour.

Mrs HULL—Will distortion of their bodies, et cetera, come in under that research?

Dr Putt—This was more looking at predatory behaviours of ex-boyfriends, or undesirable or unsolicited contact, often where they have known that person in the past.

Ms MARINO—How is this reported? What process is used to evaluate what is reported? There is a lot of it happening but it is not necessarily reported.

Dr Smith—There have been some large-scale surveys done. There are some slides in the back of the pack here that summarise those results.

CHAIR—We might finish the presentation, because some of that will be answered by the remainder of the presentation.

Dr Putt—Just to clarify one point, Edith Cowan University were focusing on young people, youth experiences.

Mrs HULL—Thank you; that is what I am looking for.

Dr Smith—In fact, most of the recent research on cyberstalking has been looking at young people. The slide I have here looks at some of the reasons why things are changing in the cybercrime world. Obviously there is globalisation. New economies in China and India are creating particular risks, not because of the types of people involved but more because of the extent of usage. There are very large numbers of people now making use of online systems. In developing countries, where people might not have the same level of resources to have secure systems in place, that can create added risks.

The user profile is changing in a number of ways. One of the most important ones is that there is an integration of computer usage in business and personal life. People are now working from home, for example, and are networked into government departments and businesses. If their home office is not adequately secured, that can create an inroad into a government department or a business. Increasing use of ICT in government creates great opportunities, largely because of the enormous sums of money that governments deal with, particularly revenue agencies, so that is a prime motivator for offenders.

In terms of technological changes, we have seen increasing use of broadband. That simply enables people to do their activities much more quickly and efficiently. There is also the trend that computers are now connected 24 hours a day. People often do not disconnect their broadband services. It sometimes creates problems if you disconnect and reconnect, so people leave them on. That means that criminals who gain access to those computers have got a much longer period of time to carry out their activities; whereas, in the past, with a dial-up service, you might only have a window of opportunity of half an hour. That is an important change.

There is an increasing use of wireless technologies. A recent *Four Corners* television program looked at the risks of wireless systems that have not been configured properly. Probably one of the greatest risks there is that of home users who set up networks following the instructions in the software they have bought off the shelf, but perhaps they might not be very technologically adept and they do not configure it correctly. That creates opportunities for people to gain access.

New methods of identification are being developed all the time. We are starting to see biometric systems, and they are also going to provide opportunities. Similarly, we now have chip and PIN credit cards and other plastic cards. While that is solving some risks, it creates others. In the UK there has been research which has shown that chip and PIN card readers are starting to be compromised by cybercriminals.

There are new payment systems and stored value cards. There are a range of electronic currencies now being used to enable people to do transactions online. In some social networking sites virtual currency is being used, such as Linden dollars. There are opportunities for people to steal virtual currency. There has been some discussion of money laundering taking place using virtual currency and theft of virtual property. There have been some cases of virtual household furniture being stolen from social networking sites and gaming sites.

Finally, there are changes in crime methodologies. Researchers have identified an important change which they have said is a movement away from syntactic attacks to semantic attacks. In the next slide I have briefly explained what those are. Syntactic attacks tend to involve the exploitation of technical vulnerabilities to commit fraud. These are things like the use of malware, skimming of plastic cards, illegal transfers of funds electronically and some of the

wireless vulnerabilities. Semantic attacks involve the exploitation of social vulnerabilities to gain personal information, and this is simply just tricking people into disclosing their personal details. Those types of fraudulent activities have taken place since time immemorial—people tricking people into giving donations to fictitious charities and other types of activities.

More recently we are seeing what we have called ‘blended attacks’, which are attacks that make use of technology to gain access to information and then use semantic means of tricking people into disclosing that information. The best example of that is phishing, which uses malicious code to establish a counterfeit website. The aim of that is really to trick people into disclosing their personal banking and other information.

On this slide I have an example of a website which is, to all intents and purposes, legitimate. Members of the committee might wish to think about the ways in which you would decide whether that was a legitimate or a phishing website. What sort of things would you look for, as a member of the public, to see if it was safe to put in your user name and password in that online banking site? As some assistance, I will direct you to the URL for the address, which uses two Vs instead of a W in ‘Bank of the west’. It is a bit hard to see from here but there are actually two Vs.

CHAIR—We are suspicious if there is no phone number anywhere.

Dr Smith—Yes; ringing up is a very useful way of verifying information. This was one example of a phishing website that was used in a study carried out by some academics a couple of years ago in which they looked at 20 websites. There were seven legitimate ones and the rest were phishing websites. Ninety per cent of people were deceived by good quality sites. Some phishing websites are obviously fraudulent but a lot of them are very good quality, such as the one I showed. Twenty-three per cent of people relied only on content to determine authenticity—that is, without looking at browser bars, status bars or any security indicators. A number of companies are now providing electronic systems to give you indications of whether you are on a real or a fictitious site.

CHAIR—I always wondered about that. For example, St George has a little lock thing on it. But, if it were a fraudulent site, couldn’t they just put a little lock on theirs, too? What does it really indicate?

Dr Smith—They do. There are more sophisticated indications that you can get. Some companies have checks in the toolbars that give an indication of your connection status, whether the site you are on is legitimate or not and whether you should proceed with a transaction. That is software that is much more effective in giving people an idea about whether they should do a transaction online. The risk is that not all computers are using those sorts of systems at the moment, and a lot of people would not even know how to make use of that.

Sixty-eight per cent of people in that short survey ignored pop-up warnings and just proceeded. Often you will have a warning come up that says, ‘Do you really trust this site? Have you investigated where it has come from?’ People ignore that and go ahead. Often the reason for that is simply this time pressure that exists in the computer world to do transactions very quickly. Part of the advice that the institute has been giving to people is to take more time in what they are doing online, to think about what they are doing, perhaps telephone the business that they are

doing a transaction with, to see if it is legitimate or not. That might take half an hour to verify what you are doing, but if you are conducting a large-scale transaction it is probably worth it.

Turning to the area of personal fraud, which is the main focus of this committee's inquiry, I think it is useful to recall the amount of information that is flowing around the world. We now have almost 1½ billion global internet users—with 16.7 million in Australia, at the last survey. We have very large amounts of data being produced, and there has been some discussion that there is in fact more data being produced than is capable of being stored—which is going to create problems in a few years. Very large numbers of people are using social networking sites and gaming sites. There are 200 million registered Facebook and MySpace users.

The sorts of information that criminals are after are really life history information—basic demographic information, government numbers, tax file numbers, drivers licence numbers and things—and financial information: bank account and card numbers and particularly PINs and passwords. Some of the high-risk activities for individuals lie in loss of laptops, datasticks and USBs. Security companies have found that those are the areas of greatest risk. It is particularly vulnerable where you have devices such as my presentation slides, which are concealed inside a pen—which is convenient and easy to use, but if that is lost there are four gigabytes of data that someone could have access to if it is not encrypted. A lot of people leave information freely available.

Sharing of personal information online: I mentioned social networking sites. Often people do not secure the information they put up. They put up too much information, there is unnecessary detail that goes on those sites. The London Office of Communications did a survey last year and found that 44 per cent of users of social networking sites allowed other people to see their personal information. Twenty-five per cent of users posted personal information openly without any password protection or anything.

One of the areas of great risk in recent years has been accidental loss of data. This can occur not only from businesses but also from government departments, particularly if you have government information kept on datasticks that are not encrypted or protected in any way. That can create a goldmine of information for criminals. There have been regular reports of very large databases having been accidentally lost or illegally given to criminals. I think the important thing to bear in mind here is that although very large databases have been lost or accidentally misplaced, we do not actually have evidence about how much of that information has been used illegally. It creates an enormous opportunity for offenders, but there is not any real research on how much, for example, of the 25 million UK residents' personal information that was lost by HM Revenue and Customs recently was compromised. Perhaps it resulted in some of the credit card scams and losses that took place in subsequent years, but we do not know.

CHAIR—When you say 'lost', do you mean that it is literally gone from their computer or that they just know that it has been accessed by someone else?

Dr Smith—In some cases it is lost as in accessed improperly. The TJ Maxx case in America involved people gaining access to that data, and it was a report in the newspapers this morning of an American suspect who was arrested over that case. But other cases involve data that is left on trains or in airports and is accidentally misplaced, and opportunistic people take it and make use of it.

A company, Verizon, does regular surveys of data breaches. In 2008 their latest survey found 90 breaches involving 285 million compromised records. Interestingly, 91 per cent of those were attributable to organised crime groups particularly operating in Eastern Europe and the United States. And confirming what we were saying before, 67 per cent of those data breaches resulted from mistakes, 64 per cent from hacking, and 38 per cent from the use of malware, so I think that the area of mistaken or accidental data loss is important.

Another way in which people can gain access to information is through buying data, compromised information, from the internet. There is an underground economy that has developed amongst cybercriminals of trading in stolen credit card information. An operation by US police a few years ago looked at 28 people in six countries who were involved in buying and selling 1.7 million credit card numbers—and over the page there is some information on the sorts of prices that have been found for different types of malware that is available for being bought and sold online. You can see that the sort of information that you need to commit a denial of service attack, for example, can be readily obtained quite cheaply—US\$100 a day to rent a denial of service attack kit, or US\$1,000 to buy 10,000 compromised PCs. Again, we do not know the extent to which these large quantities of material have been misused but the opportunities are certainly there.

CHAIR—But how do you purchase it? They are the costs but obviously you do not go down to the local corner store and do that. If someone wants to buy these sorts of things, how do they do it?

Dr Smith—Largely it is through internet relay chat rooms which have closed access—you have to become a member of them. If you get access to those then you can buy and sell online using credit cards.

CHAIR—You would be game to use your credit card in those sorts of things!

Dr Smith—A cybercriminal might not be very careful.

Mr BRADBURY—They might use someone else's credit card!

Ms REA—They must be dealing in significant volumes as there is not a lot of money being made when you look at the prices on this page. If they are going to take all the risk of being part of organised crime—as Belinda said, you just cannot walk down to the shop and advertise in the newspaper—in order for it to be viable, are they dealing in large volumes or are they taking those risks for what seems to be a relatively small amount, say, \$50 for stolen bank account credentials, for example? You would need to provide a lot of stolen bank accounts to make it worthwhile being in that business.

Dr Smith—There is a lot available that they are dealing with, so I think that is how they make their money. And the sorts of organised crime groups that are involved in trading this sort of information online are also committing frauds themselves. They are targeting consumers and businesses, so this is an extra avenue for making some money.

Ms REA—So this is a side business.

Dr Smith—There have been some very recent studies that have tried to document the extent of the problem in Australia, and I thought I would present some of the findings of these because I think it gives you a picture of just how much of a problem it is and who is getting targeted. AusCERT conducted a survey of home users of the internet. They looked at over 1,000 people using computers at home. It was a representative sample of the Australian population and looked at people aged 18 years and older with an internet connection. As I mentioned before, a very large proportion are now using broadband—84 per cent in that survey. Nine per cent of people are using wireless and smaller and smaller proportions of people are now using dial-up services. Seventy-five per cent of those surveyed had administrator rights. That is very important because that gives you access to the way the computer is configured. So if you are installing malicious code, you can only do that if you have administrator rights over a computer. It is possible when you buy your new computer to choose whether or not you want to have administrator rights. A lot of people do not make that choice and give themselves limited rights, which would be much more secure. So that is sort of an educational thing that—

CHAIR—But you can choose. You can be generally in limited use—

Dr Smith—Yes.

CHAIR—I think a lot of people think once you choose, you are stuck with it so you cannot then install software and that sort of thing.

Dr Smith—Or you can have a separate logon as an administrator.

CHAIR—Yes, but I think a lot of people do not realise that you can be normally a limited user and then switch to administrator when you need it.

Dr Smith—Yes, but for general purposes, for word processing and using email, it is best just to be a limited user. But this survey found that only nine per cent of those surveyed had done that. Seventeen per cent of people did not know one way or the other. Again, it is an education issue.

CHAIR—And I think some of the others made it up, but they knew.

Dr Smith—Yes, possibly. We can see that large proportions of people are using the standard internet security tools that are available that usually come with the new computer that you buy—antivirus protection, firewalls and anti-spy ware.

Mr BRADBURY—How effective are they? To the typical consumer, it would provide a sense of comfort that they have done what they need to do.

Dr Smith—Yes. They are not complete solutions. They certainly screen out the vast bulk of malicious code and software, but a good deal of it gets through. That is how computers keep getting compromised. You are certainly not 100 per cent secure, even if you have up-to-date software and virus protection. That is a challenge for the computer security industry to keep those protection systems up-to-date and to improve them, but unfortunately that is a cat-and-mouse game with the cybercriminals who are now devising malicious code that defeats the

security systems that are in place. So the first thing that malware does now is to try to defeat the security measures that are in the computer.

CHAIR—Sorry, what you were saying before was that even if you are not actually using your internet, but it is on, then malware or some other mechanism can access your computer, despite the fact that you are not actually using it. Is that correct?

Dr Smith—Yes, if you have a connection then there is an inroad into your computer. That will take place once some malicious software has been put in the computer that will enable an external person to gain access.

CHAIR—But what I am saying is if you are not actually using the internet, if they have not already got access, can they get access while you are not—

Dr Smith—You would need to have malware put into the computer.

CHAIR—While you are using it?

Dr Smith—Yes, but that might be an email attachment that you have clicked on six months before that has been lying dormant in your computer and will be brought to life later on.

In terms of wireless risks, AusCERT's survey found that 16 per cent of people were using insecure networks, so they are not setting up a wireless network that has been properly configured with some encryption system. Interestingly, five per cent of people admitted to using a neighbour's connection.

Ms COLLINS—Don't you need a password?

Ms REA—Not necessarily; not if it is not secure.

Mr BRADBURY—What is the main risk in this particular case? Would it be that people are using the internet at your expense? Is that the main risk, or can they do things that are more sinister than that to your computer?

Dr Smith—Someone will be using your account, so there will be a cost implication for you—they might be using gigabytes of your service. That is one problem. The second problem is that they might be moving illegal material around using your connection. They might be downloading child pornography. You would not be aware of that, except that you will have a very high usage on your broadband connection. From a legislative point of view, that is an area that does need addressing: the liability of the person whose network is being misused and also the liability of the person who is gaining access to an insecure network.

Mr BRADBURY—If that needs to be addressed, what is the position at the moment?

Dr Smith—I am not entirely sure; we have not worked through that. That is probably a question you might like to put to Attorney-General's.

Mr BRADBURY—But the point you are making is that someone could potentially have a wireless network at home that a neighbour, as in the five per cent of cases here, or a passer-by or someone who does not have permission to use that network could be using your internet connection and downloading illegal material. Obviously if that is material that is coming to the attention of the authorities, there could be some question as to who has actually done that. Is that something that you can determine? Can you trace or work out exactly who was involved?

Dr Smith—Yes, it can be traced, but there is a potential chain of liability. It could be the person who is—

CHAIR—You would be an accessory for allowing them to use your broadband?

Dr Smith—Possibly.

Ms REA—How would you know that they did it without your permission?

CHAIR—You could claim that they did.

Dr Smith—Also, there is the question about what you have authorised people to do by having an insecure network that you are using. Are you impliedly allowing anybody to make use of it just by creating it or is there some implied limitation on the consent you are giving to external people to use your network only for legal purposes? Also, what is the liability—

Ms REA—It is a bit like a credit card, isn't it? If it is stolen but you do not report it as stolen, how can you prove that the person using it is doing it without your consent or permission?

Dr Smith—Yes. And ISPs—

Mr BRADBURY—Is it difficult to configure these wireless networks in a way to—

CHAIR—Have you got one?

Mr BRADBURY—No.

Dr Smith—It is quite simple. It is not something that my aged stepmother would do very easily—

Mr BRADBURY—I am sure she has many other talents.

Dr Smith—She does. I think there is a need for both the manufacturers of hardware and software and also the companies that are advertising and profiting from these systems to make it easier for people to set up systems securely and to monitor them. It is quite difficult.

AusCERT's survey also had some figures on the extent of malware that they detected. Fifty-three per cent of people had malware that had been detected but quarantined by the software in the systems and 23 per cent had malware infections that were not quarantined, so they were live and able to be used by criminals.

Some 11 per cent of users had been notified of an infection by a third party—so maybe their service provider or someone else, police perhaps. This means that those 11 per cent did not even know that they had a problem. Some 39 per cent of people had malware only once. Some 23 per cent had it two or three times and nine per cent had it four or more times over the preceding 12 months. Worryingly, 14 per cent of people took no action to repair or remove malware on their home computers. So either they did not know how to deal with it or perhaps they could not afford to take it to a computer repair person to fix the problem.

CHAIR—Is that of the 23 per cent of people who had infections that were not quarantined—so it is a subgroup of that?

Dr Smith—Yes. In terms of risky online behaviour, of the people who said that they do click on links 32 per cent of those had malware, and 19 per cent of people who said that they did not generally click on links had malware. So people who have a high-risk behaviour in that they tend to click on links in webpages are more likely to have problems.

The most authoritative survey that has been done in Australia of personal fraud risks is the one done by the Australian Bureau of Statistics last year. That was a very large-scale survey with over 14,000 individuals surveyed. They participated in telephone interviews. People were asked about their experiences from 1 July 2006 to 30 June 2007, so the information is slightly dated now but it is still the most up-to-date that we have. They asked questions about exposure to scams—so that is receipt of an invitation, such as a Nigerian email—and the extent of the victimisation, so whether people supplied information or money and how much money people actually lost. That was the definition of scam that was used in the survey.

The results are as follows: the top line result is that five per cent of the Australian population are being victimised by either scams or identity fraud at the moment. The numbers in the boxes on these slides indicate the extrapolated numbers for the whole of the population. So approximately 800,000 Australians would have been victimised in that 12-month period. Some 453,000 people would have lost money, with total losses of \$977 million or mean losses per person of a bit over \$2,000. You can see on these slides information on the different types of scams that people said they had experienced.

Mr BRADBURY—What are the chain letters?

Dr Smith—Chain letters are like the old-fashioned letter that you received in the mail asking you to pass on the letter to someone else in return for a fee.

CHAIR—Do they actually have to pay for that? I have received some chain letters but they do not actually pay any money.

Ms REA—No, they just say, ‘Email 50 friends and if you do not then something dreadful is going to happen.’

Mr BRADBURY—So these are schemes where there is an expense involved, but there is no inherent danger with those ones that people get.

Dr Smith—Except that it is creating a lot of information that is being gathered in one place that can be misused if that is the motivation behind those.

Ms REA—With those 329,000 people who are victims of scams, is that over 300,000 people who have actually responded to the Nigerian email?

Dr Smith—Yes, they have given out personal information or given money.

Ms REA—That is just extraordinary.

Dr Smith—The benefit from the criminal's point of view is that very large numbers of these emails can be sent out—hundreds of millions of invitations go out. If you have a one per cent response rate then you will still get a lot of people.

Ms REA—That is what I would have thought—the only reason you keep getting these emails is that they send them to literally hundreds of millions of people across the world, and only three or four may respond. But I am stunned that that many people in Australia alone would actually respond.

Ms MARINO—I do not know what the demographics—the age groups—are there, but I have come across a number of seniors who are using the internet for the first time who are not aware of the risks, and more and more seniors are using the internet as a form of communication. I would be interested to know the age groups of those who are most susceptible or who are responding in that way so we know where the biggest issue is, because I think communicating the risks to that particular demographic is important.

CHAIR—Would you have that?

Dr Smith—Yes. We have done research on that. Unfortunately, it seems that all demographics are pretty much equally at risk. Different age groups might have different vulnerabilities to different types of scam. An older person who has lived a full and informed life might be aware of the risks in a financial advice or housing repair scam, a conventional type of fraud, whereas a young person might not be as risk averse to those types of scams. Younger people might be more at risk of lottery or dating scams.

Ms MARINO—Even something that looks like a body they are used to donating to, like the Red Cross. It is that sort of request, where they perceive an inherent obligation.

Dr Smith—Yes. A lot of these scams are now becoming much more convincing in the way that they set them up, and the offenders in fact gather more personal information to target people individually so that they are more likely to be successful.

CHAIR—Just on that issue of targeting, are they sending out the emails knowing that it is actually an account, or is it a random sending-out to thousands of potential addresses and then striking some that are real accounts? Do they know there is a person with that account?

Dr Smith—In the past it has been random. They just send out hundreds of millions of emails.

CHAIR—Trying almost every letter and every—

Dr Smith—Yes, or they buy databases of names and addresses and send them out.

CHAIR—So it is not random if they have your name and address already.

Dr Smith—No. In recent times, emails are being sent to targeted lists of people, so you know that you are sending it to an older person at a particular address who might have a particular vulnerability. There is also what the Americans have called ‘sucker lists’, lists of people who have been defrauded. Their information is kept on databases which are sold to criminals—

CHAIR—That is just so terrible.

Mr BRADBURY—If they fell for it once—

CHAIR—So people who have been damaged already are more likely to be approached again.

Dr Smith—So we have a re-victimisation problem.

Mr BRADBURY—But what do we know about the source of the crime that is occurring here?

Ms REA—Yes, that is a good question.

Mr BRADBURY—A lot of the material talks about Russian gangs and things of that nature. Do we have a sense of where these criminals are conducting their activities?

Dr Smith—There is limited information. The most quantitative comes from the Anti-Phishing Working Group, which is a conglomerate of businesses, set up to respond to phishing attacks. They keep statistics on where phishing websites come from, what brands are involved and who is doing them. So that information is available. They have also got league tables of the countries which are most likely to be involved in creating phishing websites. In the past, the United States was the top-ranking country. It moved to China for a while, but it is back with the United States now.

The other source of information is law-enforcement investigations that have taken place and successful cybercrime prosecutions. They have shown that a lot of serious, organised cases are involved in Eastern European countries and also America. They are the main ones. There have been quite a few cases from South-East Asian countries in recent years, mainly credit card related scams as opposed to hacking, virus or malware cases, but it seems that America and Eastern Europe are still the home of the serious, high-level cybercrime activities. But I would caution that the evidence base is limited.

CHAIR—A couple of incidents have been reported in New South Wales recently where they used computer phishing to get a whole lot of fake cards and actually produce the cards. Then a gang comes down from South-East Asia and uses all these fake cards that have been created using the information that has been phished.

Dr Smith—Yes. There was a successful operation in South Australia a few years ago where a group like that were followed and arrested. That is the risky end of cybercrime activities, where you have to actually get the cash out of an ATM and take it home with you. As long as you stay in the cyberworld, it is much more secure.

CHAIR—We are going to get a bit short of time, but there is a very important question for me that I wish to ask. One of the issues that worry me is: where can people who have been approached in this way or been the victims of cybercrime go for it to be dealt with? I had a really bizarre email with no name on the top saying, ‘We know where you live and where you work; if you want to stay safe for the next 24 hours, send me X amount of money.’ I did not take it very seriously, but when I tried to investigate who I should pass it on to there really was not anyone. The only suggestion was, ‘Ring up your local police station.’ Let me tell you: if I rang up Joe Plod at the Gosford station, they would just say, ‘Well, what do you expect me to do about it?’ So are you aware of what people can do to report it or have it dealt with? Even if they are defrauded, particularly of fairly small amounts, there does not seem to be anyone who is really interested in dealing with it.

Dr Smith—Yes. There are probably too many agencies involved in handling these sorts of issues. There are police; there are consumer affairs agencies.

CHAIR—But the police do not really deal with it; that is exactly the point I am making. They do not.

Dr Smith—They gather the information. Where there is enough evidence to mount a prosecution, they certainly will take action. There have been a number of successful cases where criminals overseas have been targeted.

CHAIR—That may be the case for very large amounts, where they are interested, but for someone who has lost \$100 or \$1,000 that is not going to go to the detectives down at the central station, and there is no way that the local police are going to have the know-how and capacity to track down whoever it might be.

Dr Smith—That was the reason for setting up the High-Tech Crime Centre a few years ago: to coordinate the information that is coming in so that all of those hundreds of small cases involving small amounts of money would go to one place, and then you would be able to see patterns emerging and put police resources into it. But there is a problem in coordination, particularly where people report these sorts of cases to multiple avenues. They will go to their banks, card issuers, consumer affairs agencies, state and territory police and the Federal Police, and also places like ASIC and the ACCC. So there is a great need for coordination of information.

CHAIR—So do you think there should be a central point for reporting?

Dr Smith—There have been proposals. We have suggested that in the past. There are central reporting agencies in the UK, the US and Canada now for computer crime. If they are adequately funded, I think they can make some inroads into solving some of the problems.

Dr Putt—That is something that has emerged in work that we have done in previous years: that issue around capacity to respond. Even where there is reporting and assuming that it is done more effectively—centralised in some way—what capacity is there to respond? Clearly, a challenge for law enforcement is having the resources and skills to detect and investigate these sorts of criminal activities. As you can imagine, when you are competing against the private sector in terms of a very specialist skills set that is required to do forensic investigations—for example, computers—it is a huge challenge.

CHAIR—Do any members have particular questions before we wrap up? I am sorry we have sidelined your presentation a bit. Why don't we skip to conclusions just before we wrap up? First I would like to take a motion from Ms Rea to form a subcommittee to finish the meeting. That is carried.

Dr Smith—I will go to conclusions. I think it is worth recalling the level of risk involved. A lot of legitimate transactions take place online. If you look at ACPA's figures—and I understand there is a submission from ACPA to this inquiry—it is really only 0.02 per cent of credit card transactions that are fraudulent, which is actually quite a low proportion. We need to bear that in mind.

In terms of document security, chip and PIN are certainly going to solve a number of problems when they are rolled out. That is taking place in Australia at the moment. The national document verification system is important. That is where agencies which issue drivers licences and passports are able to provide a verification service for agencies which are checking evidence. There are improvements in identity cards. Overseas we are starting to see identity cards being used. I do not think they are a complete solution, because if a single card is compromised that is going to create more problems, but that is certainly one policy that is being used overseas. Improvements in biometrics are quite often very expensive solutions but they are very effective and if you have got a fingerprint or a facial scan involved that solves the problems of people forgetting passwords and PINs.

As I mentioned, some of the industry responses are important—just making it impossible for people to do very high-risk things through the software and hardware they are using. Improving monitoring of transactions, notification and blocking services that banks are now using are all important ways of acting. In terms of education, the Australasian Consumer Fraud Taskforce is continuing its activities each year to raise awareness about consumer scams.

CHAIR—Can we drop down to the legislation?

Dr Smith—The identity crime legislation that was created as a model a few years ago has now been implemented in three jurisdictions, and New South Wales is considering a bill at the moment.

CHAIR—Can we get copies of all those bills?

Dr Smith—That is the detail of the Victorian act.

Ms REA—We have not got time for the detail now. We need to wind up.

Dr Smith—I will just mention the idea of the certificate which courts can issue to prove that a person has been defrauded. I think that is worth considering. Finally, there is a need to improve some of the research and statistical information that is out there.

Ms REA—Thank you so much.

CHAIR—Thank you very much. I am sorry that we took up your time and made it a bit difficult. We have question time shortly and we get spanked if we are not there! We very much appreciate your evidence. It was very interesting.

Dr Smith—Thank you for the opportunity.

Resolved (on motion by **Ms Rea**):

That this subcommittee receives the presentation of slides used by the Australian Institute of Criminology as an exhibit for the inquiry into cybercrime and authorises the exhibit. The subcommittee authorises publication of the proof transcript of the evidence given before it at public hearing this day.

Subcommittee adjourned at 1.49 pm