



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

**HOUSE OF
REPRESENTATIVES**

STANDING COMMITTEE ON COMMUNICATIONS

Reference: Cybercrime

WEDNESDAY, 21 OCTOBER 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, 21 October 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: Mrs Hull, Ms Marino, Ms Neal, Ms Rishworth

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) The 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

**MATTHEWS, Mr Bruce David, Acting Executive Manager, Strategy and Coordination Branch,
Australian Communications and Media Authority 1**

**ZIELEZNA, Mr David Ian, Senior IT Technical Officer, E-security and DCNR Section,
Australian Communications and Media Authority 1**

Committee met at 12.40 pm

MATTHEWS, Mr Bruce David, Acting Executive Manager, Strategy and Coordination Branch, Australian Communications and Media Authority

ZIELEZNA, Mr David Ian, Senior IT Technical Officer, E-security and DCNR Section, Australian Communications and Media Authority

CHAIR (Ms Neal)—Thank you very much for attending. We are very pleased that you have made yourself available to come along today. 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 in much the same respect as proceedings of the House. The giving of false or misleading evidence is a serious matter and may be regarded as contempt of the parliament. At the conclusion of your evidence, would you please ensure that Hansard has had the opportunity to clarify any matters with you before you leave. Would either or both of you like to make an opening statement?

Mr Matthews—I would like to make an opening statement, thank you. I welcome the opportunity for the ACMA to appear before this committee. The inquiry is welcomed by the ACMA as it provides the opportunity to examine the nature and extent of cybercrime occurring in Australia and the mechanisms by which this crime is perpetrated. It also provides an opportunity to assess the potential exposure of Australian internet users to cybercrime and to examine the ways in which this exposure might be reduced. The ACMA submission to the inquiry was structured around the Australian Internet Security Initiative, which is a program that provides daily reports to participating internet service providers identifying compromised computers residing on their networks. The term ‘compromised’ in this sense means computers on which malicious software, otherwise known as malware, has been surreptitiously installed without the knowledge of the computer owner. These computers, usually referred to as bots, are generally aggregated into the networks of computers known as botnets, which are controlled remotely and used for various harmful and illegal purposes, on which I understand the inquiry has been previously informed.

AISI reports are provided so that internet service providers can contact their customers and inform them that a compromise has occurred. Until contacted, the computer owners generally have no knowledge that their computer is compromised. There are a few important points to make about the AISI. Firstly, participation in the AISI by internet service providers is voluntary. Some 71 ISPs are currently participating in the initiative. Their names are listed on the ACMA’s website. The number of ISPs participating in the AISI has progressively expanded since the trial of the AISI was first launched in November 2005. It is estimated that these ISPs cover more than 90 per cent of the Australian residential internet customer base.

Secondly, I turn to the development of the AISI group from the ACMA’s anti-spam activities. The approach adopted in combating spam in Australia includes a five-part strategy involving legislation and enforcement, education and awareness raising, technological solutions, partnerships with industry, and international cooperation. The AISI program contains most elements of this strategy with a particular focus on trying to address spam at its source as the vast majority of spam is sent from compromised computers.

Thirdly, the AISI program is a unique initiative in which there is considerable international interest. The software to run the AISI was developed by the ACMA in house and is in a constant state of evolution as we seek to improve its operation. For example, since our submission was made to the inquiry we have introduced separate fortnightly reports to ISPs that identify repeated sightings of individual IP addresses over the previous month. These reports will generally correspond to the same customer and thereby enable ISPs to identify the worst offenders residing on their networks. The ACMA submission reported that in June 2009 the ACMA was reporting more than 10,000 individual compromises per day to Australian ISPs. While the number of compromises reported per day has slightly abated since that time, the botnet problem on the Australian internet remains of considerable concern. The problems in accurately identifying the number of bots on the Australian internet are detailed in the ACMA submission, but the analysis indicates the number of Australian computers that are, or have been, compromised is certainly large enough to warrant the attention of this inquiry.

The ACMA submission also sought to explain in some detail the consequences of a computer being compromised, as these consequences often have repercussions extending well after the compromise is rectified on the computer. This is because the malware that enables a computer to become part of a botnet and cause problems to other internet users usually also enables the harvesting of personal data from that computer. This data includes credit card details, full name, date of birth, passwords and user names for undertaking online transactions, records of websites visited, and numerous other forms of personal information and communications.

The final introductory point I would like to make is a more positive observation, which is to congratulate the ISP industry on their voluntary participation in the AISI. In addition to participating in the AISI, the Internet Industry Association is currently developing a voluntary e-security code of practice that seeks to develop a structured framework for ISPs to follow in responding to compromises occurring on their networks. This should result in positive outcomes to consumers as it should lead to greater industry efficiency in dealing with these compromises.

CHAIR—Did you want to say anything more?

Mr Zielezna—No, thanks. We will go straight to questions.

CHAIR—I assume the ISPs that you are monitoring are only those physically located in Australia?

Mr Matthews—That is true.

CHAIR—You say that you report to the ISPs about computers that are compromised on their network. Is there any understanding between yourselves and those ISPs how they will actually respond to that? When you say that they are participating in a trial, does that mean that they have just agreed to receive the information or they have agreed to take particular action once they receive it?

Mr Matthews—I will answer the second part of your question first. The trial commenced in, I think, November 2005, and six ISPs participated then, including large ones such as Telstra and Optus. But the trial was assessed the following year and it was determined to go to a full-blown implementation of the AISI, so we are no longer in the trial period. We certainly expect that ISPs

should contact their customers and advise them of the compromise that has been identified. Our reports provide generic information on compromise types and we expect that the ISPs should pass that information on to their customers, but it is a voluntary scheme so it is up to the ISPs to determine the best mechanism for contacting their customers themselves. We know that ISPs use different mechanisms for making contact. Some of the smaller ISPs will ring their customers and tell them that they have a compromise. Other ISPs will notify their customers via email that they have a compromise. Some ISPs will disconnect their customers when they receive a report from us, which requires their customer to actually ring the customer help desk to be reassigned a new password to access the internet. So the customer is informed at that point that they have a compromise.

We do not set out to undertake a customer focus ourselves in terms of interacting with the customers with the compromises, but we occasionally get contacted by customers who have said that their ISP has told them that they have a compromise and they want further detail themselves on the nature of the compromise. They may have taken action to disinfect their computer, but we are still reporting them as compromised, and they cannot understand why. So, on those occasions we will try to gather further information to assist rectifying the problem on the computer, and on most occasions we can do that.

CHAIR—Are you saying that if the ISP did nothing, although many do contact, when you provide them with that information they would not be in breach of any agreement with you?

Mr Matthews—That is true.

Mrs HULL—If an ISP continually flagrantly breaches that and does not shut down a site or do something, if it has an account with a consumer and the ISP repeatedly fails to take remedial action, do you have any power to enforce that?

Mr Matthews—No, we do not. It is a totally voluntary scheme, and ISPs are not required to be part of the scheme to begin with. We cannot require them to take any particular action. That is the nature of the scheme.

CHAIR—If it wanted to, the organisation could make it a requirement of participation that they actually take action?

Mr Matthews—We could, yes, but we have not taken that path of action. I think it is also worth mentioning that some ISPs use our data to correlate it with data that they obtain themselves, and they will look for multiple sources for evidence of a particular compromise occurring. They may take action that best suits their own internal arrangements for dealing with their customers.

Ms RISHWORTH—Is there a best practice model of what should be done, though, if they find a compromise? Is it shutting down or is that just creating too much hassle? Is it sending an email? Is there a best practice? What would you see as the best way to get through to the customers?

Mr Matthews—I think in an ideal world it would be best to ring the customer and tell them that they have the compromise, but that is not economically feasible given the quantum of

reports that we are providing each day. Some large ISPs get in the order of 2,000 reports per day, and it is a significant burden upon those ISPs to contact their customers in that way. A good model for those large ISPs I think is to contact their customers via email and monitor them to see that they have taken action. Some ISPs will have an escalated procedure whereby, if the customer is reported three times, for example, within a certain period, they will disconnect their customer from the network and get them to ring in and receive further information. Some customers in isolated circumstances have had their accounts terminated by ISPs for not taking any action. Some ISPs also have a different method, which I think is certainly worth examining, and that is they will place their customers into what is called a walled garden; that is, they cannot obtain access to the broader internet until they have taken action to disinfect their computer. That walled garden will provide access to the software they need to fix their computer. That model is used overseas in some jurisdictions, and we see benefits in doing that within Australia. But again, it can be quite expensive to set up that arrangement.

CHAIR—What sort of proportion would there be of ISPs that do not take action? Are there any ISPs that have made a policy decision not to notify their customers, or is it just something that happens by error?

Mr Matthews—I could not answer that question entirely because I am not sure what all ISPs are doing in relation to the reports we provide them.

CHAIR—So, they do not even notify you whether they advise them?

Mr Matthews—We have surveyed ISPs to find out what they do, and we understand they have a variety of approaches. Certainly one ISP in that survey said they did not act on our reports individually, but they used that data to correlate with other data that they got in order to determine what action they would take.

CHAIR—It has been suggested that an ISP terminating a service as a result of being given this sort of information may lead to liabilities for that ISP. Obviously some of the ISPs do not see that as a problem, because they are disconnecting people's services. Do you think there is not a liability question for them or that they feel there could be potentially but believe that their customers will not take any action?

Mr Matthews—I am not a legal expert, so I cannot really give a definitive answer to that. I can mention that the spam code of practice, which is a code developed by the Internet Industry Association, does contain provisions that provide ISPs with the ability to disconnect their customers if they are harming the network. That code has been registered by the ACMA, and so it has that legal status of codes registered by the ACMA.

CHAIR—Could you take that question on notice? Obviously you said you are not legally qualified, but I assume that probably ACMA has made some legal assessment of that question at some stage. If you could take it on notice, and if you do have any further information to respond to that I would very much appreciate it.

Mr Matthews—I am happy to do that.

Ms MARINO—In your submission you urged a more comprehensive and timely response to compromised websites. What specifically would you like to see implemented to achieve this?

Mr Matthews—I think to begin with there needs to be a system whereby website owners become aware of the fact that their websites are compromised. I do not think all website owners are aware of that fact. I think that would be a good start in relation to addressing this problem, which is in many ways one of the most significant e-security problems on the internet at the moment. It is the main vector for infection of computers—customers or internet users visiting websites that have infected malware and that have malware on the website. It is relatively expensive to maintain a website so that it is entirely secure, and even then in extreme cases it might be possible to breach the website security. I think there needs to be a much greater focus on maintaining the e-security on websites, particularly for websites that have forms for entering data onto the website, because they are the most vulnerable to being infected. Perhaps David might like to elaborate on that point.

Mr Zielezna—Another common vector for mass infection of websites is stuff like known vulnerabilities. Somebody who knows about a known vulnerability can just put in some key word that will get Google to show them a whole heap of them that they can infect.

Ms MARINO—Sorry, what is a known vulnerability?

CHAIR—You may need to explain a bit more.

Mr Zielezna—A known vulnerability is in an exploit on a particular software package that the website uses. Somebody could use a known exploit to find more sites via Google that use that software with that exploit. So, Google can be used in that way to generate a large list of vulnerable websites that they can then compromise. There are all sorts of other similar related methods that they use to mass infect.

Mrs HULL—We have been hearing evidence from law enforcement and a whole host of areas here, and it just seems to be such an extraordinary technical issue. We have heard that the NBN is going to make it even more difficult to manage and to detect. Is there a real answer in putting together a process of rules and regulations for ISPs and whatever to start to try to ameliorate the issues here, or is it almost non-fixable?

Mr Zielezna—I do not think there are any silver bullets for the issue or any potential framework to create something like that. The issues involved are international, and the people involved, the bad guys who go and do these sorts of things, are very crafty. There is a huge financial incentive for them, so they will spend a lot of time investigating different ways in which they can cause breaches and that sort of thing. In general, the software that the public use to create websites and use in their day-to-day activities is very complex and it is hard to put in security guidelines that are always foolproof. There will always be holes in software in general, and they are the vectors that people try to exploit.

Mrs HULL—Is this the reason why the code for ISPs is voluntary? You started out by speaking about this, but I am yet to understand: how many ISPs are in Australia? I think you said you have 71 members that are voluntarily involved in the code. So, how many do we have? We

have 71 involved. Literally, why is it not compulsory to be a member of this code? Why was it set up to be voluntary?

Mr Matthews—There are a few questions there. In terms of the number of ISPs in Australia, I do not have a definitive number, but I understand it is in the order of 500 to 600. As I think I mentioned in my introduction, we believe we have more than 90 per cent of the internet user residential customer base covered by the AISI. That is because a lot of the ISPs that are not members of the AISI are very small ISPs. That figure of 71 is also in some ways misleading, because there are a lot of ISPs who have bought other ISPs who trade under one name and there may be four, five, six or seven ISPs under that company, and mostly they are not included in our list. We certainly have all the large ISPs as part of the AISI. We are seeking to expand coverage. I should also mention that we have a couple of universities who participate as well, because they have their own IP address ranges. Why is it voluntary? That is really a policy question, why the scheme is voluntary, but I should mention that, to my knowledge, there is no equivalent scheme to the AISI anywhere else in the world. In terms of an e-security code of practice that applies to ISPs, there is nothing of that nature also anywhere else in the world. I think ISPs have their own approaches to dealing with these issues. They have their own internal systems. Not every solution that might be identified would be suitable for each ISP, so they need to implement the program in the way that suits them the best.

Ms RISHWORTH—You mentioned that the ISP does notify someone that they have a compromise, and there is a walled garden system with the software to help them clean that up. I have a website, and I have a form that people fill in. If I had a compromised website that someone sent me an email about, I would have no idea how to fix it up and make it appropriate. Do the majority of ISPs instruct the end user, whether it is a website or email users, how to fix up their system and protect their computer and website?

Mr Matthews—We expect them to provide that information to their customers. A number of different websites provide advice of this nature, including www.staysmartonline.gov.au, which we recommend. We also have information on our own website. For particularly complex compromises the organisation AusCERT also has quite detailed information that can be provided. Usually the information is consistent. Some may go into more detail than other sites provide.

Ms RISHWORTH—Some ISPs hold their hand whereas others just say, ‘Have a look at these websites?’ so they vary in the amount of handholding that they do for the end user?

Mr Matthews—Yes.

Ms RISHWORTH—Would you say quite significantly?

Mr Matthews—I would say very significantly.

Mr Zielezna—In addition, we also help the ISPs understand the compromises when they are entering into dialogue with their clients.

CHAIR—In layman’s terms, how does the software work that identifies which computers are compromised?

Mr Matthews—I will give a general overview and perhaps David might elaborate. We get data from a variety of sources, and we keep those sources confidential. Some of the data we provide is on the basis that it is kept confidential. We have our own data sources as well that we have developed, but they are fairly minor part of the overall set of data that we receive. Each data source comes in a different form. The AISI is really a series of data handlers that collate the data into one central database, into a common form that we can send out a standard set of information to ISPs about compromise types.

CHAIR—What sort of people does that data come from?

Mr Matthews—It comes from organisations that are operating in the e-security area.

CHAIR—What, private security companies?

Mr Matthews—It comes from various sources. I would rather not say.

CHAIR—Really, we are asking you to say. If you want to have it dealt with confidentially, we can do that, but we really would like to know.

Mr Matthews—One of the organisations that provides us with data is the Shadowserver Foundation.

CHAIR—If you are happy to say it now, we will be on the record, and other people will be able to access it, so just remember that.

Mrs HULL—Could we not ask for the question to be answered with a follow-up paper in confidence?

CHAIR—What I am saying is we will hear now what is able to be said openly, and then if there is anything you cannot say openly, you can provide it in a written form and we can accept it on a confidential basis.

Mr Matthews—I will identify one source, which is a significant source, and that is the Shadowserver Foundation which is a group of, I guess, e-security experts who voluntarily work together to obtain data about compromises. They provide data to a number of organisations around the world. We recently hosted one of the key people from the Shadowserver Foundation in Melbourne, and we invited ISPs and other interested parties to a presentation on their operations. So, we have, to that extent, been public about our links with that organisation, although we have not identified the fact previously that they provide us with data. But there is no confidentiality issue with that organisation in relation to revealing the fact that they provide us with data. David, you might elaborate perhaps how they gather the data.

Mr Zielezna—Yes. Quite commonly the data is gathered in the form of sinkholes or honey pots or traps. Basically they are passive machines or computers or networks that are likely to be touched by infected machines like, say, the conficker virus. That very often just reports back to a command and control server or command and control network. If the good guys are able to subvert any of the command and control channels, they can then set up a sinkhole or something along those lines, which just sits there waiting to be contacted by all the infected machines. By

that means, we can identify which machines are infected, because eventually they will contact the sinkhole, and then what they are infected with can be identified by the behaviour they exhibit. That is generally how the data is gathered.

CHAIR—So, the sinkhole is a lure computer?

Mr Zielezna—Not exactly a lure; it is passive, but it is just sitting in a position that it is likely to be contacted by infected machines.

Mrs HULL—With respect to the spamMATTERS software, we understand from your submission that you have 290,000 registered users, and you have had something like 41 million reports of spam since this program began. Are you able to give us an explanation covering, firstly, how the process works, and can it get through existing filters or can it be used in place of other anti-spam filtering software? Secondly, what sorts of reports do you generate as a result of using spamware that could help us to understand the significant picture of how spammers work—whether it is directing consumers to infected websites, et cetera? Thirdly, with 290,000 registered users and over 6 million residential internet users in Australia, is there a campaign or promotion or marketing that you intend to do to get more people on board using spamMATTERS?

Mr Matthews—I will try to answer those questions in series. As to how the process works, there are two forms of the spamMATTERS software. There is software that you can download from the ACMA's website that installs as a plug-in to Microsoft Outlook or Outlook Express. Once installed, a button will appear in your email client such that you can simply select mail that you consider to be spam, click the button, and the email will be sent to the ACMA in a forensically intact manner. That means that the header information on the email remains intact, which is very useful for investigative purposes. There is also another form of the button which appears in Telstra's webmail client. We have a very large number of those 290,000 people who are registered Telstra webmail users. This is a great initiative. We get lots of very good data from that button, and we have been encouraging other ISPs as well to move into that direction and install a similar button. We hope to be successful in encouraging more ISPs to participate over time.

As to the sorts of reports we get, you are quite right; the spam that is reported by the button is quite different from the general spam on the internet. It is the spam that has transited through all the ISP's filters and any filters that may be on the software, so it is not in any way representative of spam generally occurring on the internet. I think it is useful to know what ISPs do in relation to filtering out spam at the network level. One large ISP would filter out in excess of 90 per cent of the email that they receive on their service, and it would never be provided to a customer. Most ISPs have some similar mechanism in place. That is a very rough filtering process. There will still be a lot of spam that comes through after that. Very large volumes of spam are generated through the network that never reaches anywhere near the customer. The spam that we get through spamMATTERS is used to identify particular campaigns of spamming activity. We report regularly to the Australian High Tech Crime Centre phishing email campaigns that we have identified through the spamMATTERS software.

I should also mention that we are developing a successor to spamMATTERS in terms of an interrogation system, which David and his colleagues have been working on developing, to

improve the analysis of the data that comes through. We provide reports to overseas authorities that are participating in the Seoul-Melbourne Anti-spam Memorandum of Understanding about spam that has originated from their country. We are seeking to develop that capacity in a much greater way through the new system I am talking about. In terms of the data we receive, we receive enough data, I think, to undertake many investigations. It is not a problem of not getting enough data through the spamMATTERS software.

We are really looking to identify trends within that data and also use it to extract information on what we consider to be infected IP addresses, which will again feed back into the Australian Internet Security Initiative. Again, this new system that we are developing will hopefully do that in a much more sophisticated manner than is currently done through the spamMATTERS software.

Mrs HULL—Is there a desire to do more marketing and promotion to get more residential users to participate with spamMATTERS? If you have 290,000, which seems an enormous amount, but there are 6 million residential internet users, would it not be desirable to get more on there?

Mr Matthews—I think the pathway that I would like to take in this area is to encourage more ISPs to install a spam button in their webmail systems. That is much easier to maintain. A problem with the spamMATTERS software is it is just currently available for Microsoft products. It is only available for Outlook Express and, I think, Outlook 2007. It is quite an effort to make sure that that software is compatible with each successive release of Microsoft's operating systems and also their email clients. A much better solution from my perspective is to try to get the ISPs to install a button in their webmail systems.

Mrs HULL—This committee will make recommendations in its report. Should we be considering encouraging ISPs to install this?

Mr Matthews—Yes.

Mrs HULL—So that would enable them to reach far more people in the system?

Mr Matthews—That is right. Yes, it would.

CHAIR—It would also give you a lot better data so that you are able to better identify computers that are compromised, with more information that comes in through these buttons?

Mr Matthews—That is true.

CHAIR—When you said that Telstra is using the button, do you mean BigPond?

Mr Matthews—BigPond, yes.

CHAIR—I just got BigPond homemail. I do not remember having a button on it.

Mr Zielezna—It is in your webmail when you log on to their website to use their BigPond provided email service. The button will be in there and you mark it as spam.

CHAIR—Do you have to particularly select it? It is not automatic as part of your BigPond?

Mr Zielezna—Yes, that is right. It is basically up to the user to report it as spam. That is everything that has already traversed BigPond's spam filters yet has still made it through.

CHAIR—I see.

Ms MARINO—With spamming attracting a civil penalty, have you identified or tracked down any spammers in that regard, and if so what sorts of penalties have been applied? Can you see any case for criminal penalties for this sort of behaviour?

Mr Matthews—About 99 per cent of spam, as we mention in our submission, is sent from botnets. Running a botnet currently would be captured under the Criminal Code. We liaise with police on a fairly regular basis. We provide them with information on botnet activity that we have identified occurring in Australia. In the recent *Four Corners* program, which provided detail of an AFP investigation, we were the ones who informed the Adelaide police that there was this botnet operating in that area. The adequacy of the current legislative framework to deal with these issues is really not something that I can comment on. But there is good cooperation between the e-security agencies and ourselves in relation to passing on information. We are trying to further that to the extent that we can.

Mrs HULL—When you speak of getting more ISPs involved and putting in these buttons, do you have intentions of having, say, a forum to get more ISPs involved? You have recommended an e-security forum on page 24 of your submission. Have you discussed this with the Internet Industry Association? Apart from the ISPs, who do you think would be useful people who should participate in those sorts of forums?

Mr Matthews—I hope that out of the development of the e-security code there may be the opportunity through that process to continue that type of interaction and perhaps develop into a forum where information can be shared between ISPs about malicious activity occurring on their networks. I am not aware of any current arrangement, formal or otherwise, where this interaction occurs. It is such an important issue, and ISPs are really in an ideal position to obtain this information and pass it on, that a forum should be established.

Mrs HULL—Who should do that? Should we be recommending that the departments hold these forums or is it ACMA that should be holding these forums? Who should be doing that?

Mr Matthews—I think the place to start would be to raise it through the Internet Industry Association through its ISP membership to see the way they think this would work most effectively rather than our mandating it. I think it is much better for this to develop in a cooperative manner. That would be my approach.

Mrs HULL—How do you keep skilled? How do you access the skills and the skilled people that you require to keep on top of all of the new and emerging issues and challenges that you have to face? Do you continually relook at the process of recruiting and whether you have the skills required to meet the challenges? How do you do that?

Mr Matthews—That is a challenge. I think it is a challenge for all government organisations. I feel like the AISI is a scheme that has attracted some very talented individuals who are just interested in undertaking this work. I am very pleased with the quality of the staff that we have at the ACMA dealing with this issue. I know that other agencies are certainly struggling in obtaining skilled staff, and it is difficult holding on to staff with these skills, because they become very attractive to private industry and also to other agencies. How do we recruit on an ongoing basis? At the moment we are fully recruited with the funding that we have available for this program. We intend to maintain the quality of the staff that we have just through promoting what we do as a very useful and interesting job. Perhaps David would like to elaborate.

Mr Zielezna—Quite often the people involved in the e-security industry are highly passionate about it and keeping upskilled is just something that they want to do. Even if they were not working for an organisation and getting paid to do it, it is almost certain that they would still be doing it, up to a point obviously. In terms of recruiting the right kind of people, generally the staff who already have the desired skills are the people who do the interviewing. We try to pick the people who are passionate and are going to be basically maintaining their own skill sets, although we do identify areas that we should and do work on. Usually among all of us we have the required skill sets to get everything completed.

Mrs HULL—I am curious, because it seems that the people who are most efficient and effective at putting together these spams and putting together all of these illegal activities pretty much are what we would generally call non-degreed and non-skilled people, who are just in there doing it. Do you have to have a process of formal education and tertiary degree courses or would you recruit some young 17-year-old who is pretty savvy and knows what they are doing? Do you ever consider recruiting like that?

Mr Zielezna—It is often a mix of both. Quite frequently the people who do apply and get the jobs do have degrees and formal qualifications. However, we generally look more for their actual acumen for doing all the tasks, their passion for it and their interests and related things like that.

CHAIR—It has been suggested to us, particularly by I suppose commercial companies involved in the industry or those who are affected by e-security, that there should be some sort of secure forum between government and different commercial bodies where information can be exchanged on a confidential and secure basis. In particular, banks obviously have a big interest in e-security, but do not want to be out there telling the world that they have had a compromise. Do you think a forum like that would be useful, and has ACMA given any thought to how that should be set up?

Mr Matthews—We actually participate in a forum with the banks already. The forum is called interbank. That forum has been established by the banking industry. It is not a government initiative. I think we are the only government agency on that forum. We certainly keep up our skills and information through interaction with that forum, and it is very beneficial. The Australian banks I think are doing a very good job in establishing that committee to share that information. When the forum meets, it will usually have a morning session, which is open to ourselves and maybe they might invite other non-bank organisations to attend.

Mr Zielezna—Often law enforcement.

CHAIR—Yes. I think what was being suggested—and I gave banks as an example because they are very obvious—was that it be a forum wider than just the banks, and really anyone who had an interest in e-security or could contribute information in some way; that they might be represented in that forum.

Mr Matthews—For me to comment I would probably need to have a better understanding of the purpose of the forum.

CHAIR—I think it is essentially to have as much up-to-date information available to everyone involved in the area, so that obviously the best steps to combat cybercrime can be taken and to protect I suppose both government and commercial entities who might be compromised by that sort of activity.

Mr Matthews—There are already a lot of informal networks in place, and groups where e-security experts—the passionate people that David was talking about—share information. They are a very effective mechanism for sharing information. We use those networks to shut down sites overseas. They are international groups. This is an international problem. They are quite informal. They work very effectively. I think they are a very good model for taking this forward. Also in the spam world we have a group called the London Action Plan, which is made up of about 90 organisations, including government bodies, organisations like Microsoft and other anti-malware vendors. Again, that is an informal forum where information gets shared very quickly and is very useful for investigations. I think certainly the more that those sorts of forums can be established, the better.

Ms MARINO—You are involved with that. Are there any barriers that you see to your involvement with those types of agencies?

Mr Matthews—Which agencies, sorry?

Ms MARINO—With respect to who you are talking about now, are there any barriers for you to be able to engage with those and share intelligence or information, either here or internationally?

Mr Matthews—There would be certainly restrictions on sharing certain types of information. To enable the sharing of information in relation to spam investigations, for example, we have signed a memorandum of understanding with different countries to assist that information sharing. That is the more formal detailed information of a much more personal nature. We have a number of those MOUs in place. Apart from the informal sharing of information, there are no impediments that I am aware of.

Ms MARINO—Do you have any recommendations for us on a process or other that would assist you in working with overseas agencies, regulatory bodies or others?

Mr Matthews—No, not really. We have a fairly good relationship already with a number of overseas bodies. It is really having the time to undertake all those interactions that is perhaps more at issue.

Ms MARINO—Is that an issue of staffing?

Mr Matthews—It is an issue of staffing in terms of being able to maintain these contacts, yes. There are finite resources. For example, we do not undertake any action in relation to reporting infected websites to website owners. We do not have a direct remit for doing that. We have occasionally reported them where we have identified them, but we have not undertaken action in that area because the resources for doing that are quite substantial. There are a number of different ways we could allocate our resources, and it is just a matter of determining priorities. We have been given funding to undertake the Australian Internet Security Initiative, so that is where we focus our attention.

CHAIR—There has been some suggestion that it is quite difficult for particularly individuals to have action taken on cybercrime, particularly because there might be individuals anywhere of course, and it may be relatively small amounts of money. Essentially there is a central point if it is a very large amount of money or something major, but if you are, say, Mr and Mrs Bloggs who have lost \$100 because of some cybercrime scam then it is suggested that you go to the local police station. Not many local police are very well equipped, even if they are willing, to be able to investigate that sort of offence. It has been suggested that there should be a central point for reporting cybercrime. McAfee appeared before us, and they have been involved in setting up a cybercrime portal where, as they described it, people can obtain information about cybercrime and what steps they can take to make their computer more secure. Also, they could put their information there about what has happened, and that will essentially refer it to the appropriate body to deal with that issue. Is that something that ACMA has looked at or is considering? Has any policy position been taken in regard to that sort of proposal?

Mr Matthews—It is not something that the ACMA has looked at. We do not have a direct enforcement role in relation to the Criminal Code for these sorts of e-security issues. Our legislative involvement is through the Spam Act, which has a civil penalty regime. A general response to your question—I think it is a very good idea. The more efficiently we can coordinate the transmission of this information the better it is for all agencies that are involved. I would certainly personally support that recommendation.

CHAIR—There is often a bit of a blur between what is civil and what is criminal, and what is not a crime at all. Many people who are affected may not really know exactly where they fit in, which is why it is so hard to report.

Mrs HULL—Having said that, AusCERT has said that the model the Japanese run is much stronger than what they call Australia's more fragmented approach. Is there a case for Australia considering combining the efforts into a single centre for users to make disinfecting machines? We are talking specifically about Trend Micro, under the Japanese cert, which has a cyber clean centre analysis test, et cetera.

Mr Matthews—Yes.

Mrs HULL—Do you have a comment on that? Is there a case for Australia to have a combined centre at one place?

Mr Matthews—I think a portal is a good idea, which is in a sense a combined centre where you can divert information to the relevant areas. I am aware of the program that you are referring to, which is operated by the Japanese government, where they provide a CCC, a Cyber Clean

Center. They also provide software whereby somebody who has an infection on their computer can download this software for free, and it will disinfect their computer. It may not clear all the infections. I think that is a very good initiative.

Mrs HULL—So, it would make sense for us to consider that in our report? It would make our system much stronger to have that single area and to follow a similar guideline, perhaps not the same but certainly it might be a one-stop-shop where you can get software that can disinfect?

Mr Matthews—I think that would be a good movement. I am not sure that any software is going to ever be able to disinfect everything, but certainly software is very important in part of the overall approach to this problem. Of course, there are many economic competitors in what is a very large industry, the anti-malware industry, and they may also have views on such a centre in relation to their own activities.

CHAIR—Thank you very much for coming along. Again, it is very much appreciated. If there is anything you want to add on the issue of your sourced information that you wanted us to receive on a confidential basis we would be very happy to receive that from you.

Mr Matthews—Yes. We will certainly provide you with some information.

Mrs HULL—Including what you think the committee should recommend.

CHAIR—I think that is our assessment.

Ms MARINO—Not necessarily related to this, but in your view what is the No. 1 concern in relation to cybercrime?

Mr Matthews—I would say infected websites at the moment.

Committee adjourned at 1.36 pm