

WEDNESDAY 25 NOVEMBER 2009

Present

Garden of Frogmal, B
Hannay of Chiswick, L
Harrison, L
Hodgson of Aston Abbots, L
Jopling, L (Chairman)
Mawson, L
Richard, L

Witnesses: **Mr Chris Gibson**, Chief Finance Officer, Forum for Incident Response and Security Teams (FIRST), and **Mr Andrew Cormack**, Chief Regulatory Adviser, JANET (UK), examined.

Q48 Chairman: Can I say to our two witnesses, Mr Cormack and Mr Gibson, welcome. It is very good of you to come, we very much appreciate it. As you know we are in the early stages of our inquiry on protecting Europe from large-scale cyber-attacks and we are very much looking forward to hearing what you are going to say to us. Perhaps you would like to begin by introducing yourselves if you would because we have just been asking ourselves what JANET means and also FIRST which we have had explained to us. It might be helpful for the record if you would introduce yourselves please. Mr Gibson.

Mr Gibson: Thank you very much for inviting me to come here; I am very glad to come here, it is certainly very interesting. Chris Gibson; I am the Chief Financial Officer of FIRST which is the Forum of Incident Response and Security Teams. FIRST is very much a forum, I would emphasise that fact, there is no standard FIRST view on things, it is very much a grouping of teams, people very disparate in multiple communities, multiple constituencies. I have been the finance officer for a number of years now; I have been involved with FIRST for ten years and I would like to hope that I could bring something to the table in terms of the

general view but it cannot really be said to be the FIRST official view. I work for a large multinational bank, that is my day job, but this is something that we as a bank are a member of, we have been in there for a number of years and we think it is extremely valuable for the incident response community to bring people together, to talk about incident response and so on, so that is what we do. We are a US non-profit organisation, we have very much educational outreach, bringing incident response teams together and making the Internet a safer place is our watchword.

Q49 Chairman: Thank you. Mr Cormack.

Mr Cormack: Andrew Cormack. JANET was originally the Joint Academic Network. We are the UK's education network and we connect all universities, colleges, regional schools networks and research organisations together and to the Internet. As far as they are concerned we are the Internet so we are a large computer network and, depending on how you count potential users, our marketing people have recently suggested up to 16 million people in the UK use JANET either as school pupils, as students, as teachers or as researchers. Most of them are probably unaware that we exist because they will see their school, college, university network, but the way that those organisational networks are connected together and to each other is us. We are probably, in terms of infrastructure, equivalent to large corporate organisations, telcos, and the capacity of our backbone is equivalent to any of the national telcos, it is a very large network. I have worked there for just over ten years. For the first three and a half of that I ran the incident response team for the network so we as an incident response team were members of FIRST and in fact we still are. Since then I have moved into more of a policy regulatory role (as indicated by the job title) but I am still very much involved in international incident response discussions. I was invited to become a personal member of FIRST after I had ceased to be a member as part of the team. Also, at the request of the European incident response teams, I have offered to be a member of the permanent

stakeholders group with ENISA and I have been doing that for five years now. I am also a member of the TERENA European incident response group. The other relevant thing probably is that for the first year when I worked for JANET we operated a pilot of a pan-European incident response team for research and educational networks to find out how effective that was. Possibly the fact that the pilot only lasted a year after I joined it indicates how successful it was. Unfortunately we could not get sufficient agreement on what such a team should do to justify continuing funding for it, but it was an interesting experiment and the lessons were useful.

Q50 Chairman: Thank you very much indeed. You both realise that this is a Sub-Committee of the European Union Select Committee and a number of us are members of that umbrella committee as well, and that means that all the activities of that Select Committee and the Sub-Committees are involved with European Union affairs. To what extent do you believe that Internet resilience is an appropriate topic for the European Union to tackle and get involved with?

Mr Gibson: I believe it is certainly of value. I certainly believe that the European Union has a role in expediting and jump-starting, so to speak, incident response teams, but I am not sure that I would agree that a pan-European response team is the way to go. Our experience has taught us that that is not the way to go but in terms of getting teams to start building a structure, helping incident response teams to build the relationships and make the Internet a safer place, absolutely I agree.

Mr Cormack: Internet resilience is not something that any country can do on its own. The idea of the UK Internet is technically meaningless, we are so intertwined with other countries' networks through large companies, through telcos, just through the way that networks happen to be connected. Incident response eventually is something that will need to be done globally in terms of teams globally working together to fix problems. One thing we have found is that

regional activities are actually a very good place to discover good practice. There are very simple pragmatic things like it is quite easy to have a meeting of European CERTs, we are all within a couple of hours flight, we are all within two time zones – plus Iceland which is in another time zone – and what has happened over the past four or five years is that there is a European CERT activity, there is an Asia-Pacific CERT activity, there are some joint activities in the States. Each of those is focusing on particular issues of interest to them and the other regions can then learn a lot from those. We have done a lot in Europe on training which Asia-Pacific and South America through FIRST are picking up on; Asia-Pacific have done quite a lot on exercises, particularly around the Olympics, and they are passing that information on to us so it is a good way to try out ideas to find out what works.

Q51 Lord Hannay of Chiswick: Could you perhaps just say a few words about your one year's experience of getting involved at the European level which did not justify continuation of funding. What were the problems that you hit and were they problems back then or are there still problems going forward? If you could just say a few things on that it would help.

Mr Cormack: They are continuing issues. We were looking only at the research and education networks which were a handful of networks that contributed to the pilot – I cannot remember the exact number, but fewer than ten. What the pilot ended up doing was we had a desk where any national research network could send incidents or parts of incidents that it did not want to handle, that were outside its constituency. That gets less useful as teams grow and develop because they will develop their own direct connections, their direct relations with other teams in other countries, in other areas and actually inserting a third party slows things down and increases the risk of miscommunication and things like that. Once you can establish a mesh of trusted peers that is a more effective way to deal with problems. The pilot was quite good for establishing that trust because gradually the members of the pilot got to know each other better. They tended to develop at different speeds, so JANET has had a

CERT since 1984. Even then we had been in existence for 15 years; we were pretty well established and we were really just passing incidents on to the room next door as it happened, to have them dealt with through their workload. Other countries were interested in whether a pan-European team could provide them with out-of-hours cover because that was something they wanted; we were English and Croatian-speaking as it happened and we could not provide out-of-hours cover or first line support for a Spanish network in Spanish and to cover all the nationalities with a level of knowledge and understanding of their communities that you need would not have been feasible, and there would not have been much interest by other countries in funding that. At the time it was a difference of expectations, plus this fact that actually there is a better way of doing it which we did look into.

Q52 Lord Richard: I am simply wondering whether “resilience” is a term of art or does it mean what we all think it means?

Mr Cormack: I would say that most people understand the same thing by it until they actually want to sit down and define it, at which point there are a lot of variations.

Q53 Lord Richard: What do you mean by it?

Mr Cormack: I would mean by it the ability to not fail catastrophically under an incident, under attack, under natural disaster. A resilience network can degrade but it should do so in a relatively benign fashion.

Q54 Lord Richard: Capacity to resist.

Mr Cormack: Capacity to resist.

Q55 Lord Richard: And survive.

Mr Cormack: Yes, but those who demand that resilience means that an attack on a network is completely invisible to its users are setting too high a barrier and I do not believe we can do that.

Q56 Lord Hodgson of Aston Abbotts: My Lord Chairman, I wonder if it might be helpful if I took question 7 here because we are onto the local or global straightaway and we are in danger of re-ploughing the field a bit later. My question is about local and global and whether drawing up plans at an EU level makes any sense – which you have been partially answering – or whether we should be immediately involving the USA or Russia and others. We have had some interesting evidence from the Chairman of the Board at Arbor Networks in which he says that none of the Internet’s problems respects national boundaries and talks about the need for international co-ordination. “Such teams need to be allowed to freely communicate with their peers in foreign countries. At present, barriers exist between allies that prevent information sharing at the pace that is needed, of the order of minutes and not weeks.” Could you say a bit more about that and the global local issue and what are the barriers that are preventing collaboration and, indeed, is such collaboration a good idea?

Mr Gibson: I personally believe that collaboration is very much what FIRST was set up to do and that is what we have always aimed for, we have brought in teams from China, from Russia, from South America, North America, India et cetera to bring them together to enable them to build those relationships. As a member of a large bank when phishing first started hitting us we would ring up people in China and get absolutely nowhere because we would be talking to an ISP in China, the wrong time zone et cetera, et cetera. Once I had met people through FIRST who worked for the Chinese team and I had shaken their hand and bought them a beer I was able to get a very fast direct line on something and get things done, whereas going the official route – I could talk to the NHTCU for law enforcement or I could get my US counterparts to talk to the FBI and it percolates across. It just takes too long, it is very

bureaucratic and my personal view is that that personal interface, the fact that I have met them and talked to them and so on is absolutely crucial. That is where I am very loathe to look at things like formally saying it is a European problem, you have to go this route, through a European group, across the water to an American group, down the chain there, I do not think it works, especially for an international bank. We are in 100 countries and the thought of having to channel an incident in Europe this way and an incident in America that way just does not fly, it would not work.

Q57 Lord Hodgson of Aston Abbotts: The barriers that you think are being referred to in this paper are bureaucratic barriers.

Mr Gibson: I believe so, yes.

Q58 Lord Hodgson of Aston Abbotts: Not legal barriers, just organisational obstruction.

Mr Gibson: I think so, that is my gut feeling.

Chairman: Lord Hodgson, you will have the opportunity on 9 December of pursuing this further because Arbor Networks are coming in to give evidence to us at that time. Lord Mawson?

Q59 Lord Mawson: Thank you, my Lord Chairman. What does a CERT have to do and could you give us some practical examples?

Mr Gibson: It very much depends on your constituency. The CERT that I belong to in my day job so to speak is a bank. We look after any kind of information incident within the bank and that could include faxes being sent to the wrong fax number, which in Japan is an issue because of the privacy laws. It can involve someone trying to hack into our network, it can involve someone internally trying to break into systems, it can be a multitude of things and we encompass that under SIRT (Security Incident Response Team). We call it that rather

than a Computer Emergency Response Team because we try and cover all of the information leakage issues through that – such as someone putting people’s personal data in a folder and dropping it in the trash can outside the office because they cannot be bothered to shred it and so on. We try and encompass everything. To us any incident is a very serious incident, we are a bank and we have, obviously, a vast amount of electronic information and any incident, anyone breaking in or any information leaving our business is remarkably serious and gets escalated a long way up our management chain very quickly. That can be very different to, say, a university network. We own the computers on our network, we control them, we can make sure they are patched et cetera et cetera; in a university you have a crowd of people turning up with their own computers that may be patched, may not be patched, it is a very different ballgame, so to try and say a CERT is this and neatly encompass that in a three line sentence is a very difficult thing to do.

Mr Cormack: I accept that. I was trying to generalise, knowing that I was going to be sitting alongside Chris who has actually got a very nice example of the breadth because JANET’s CERT sits in the network operator. We have no ability to see individual machines – the laptop that is sitting in my bag will be within the constituency of JANET’s service at the moment but they have no authority over it, unlike Chris who I imagine can seize any machine, shut them down, kick them off, do what they like. I think the general thing that a CERT does is it receives reports of incidents, it then understands what is actually going on to the best of its ability and it then passes on relevant information to the people who can make the incident happen. That is the only standard thing.

Mr Gibson: Within the context of its organisation I suppose.

Mr Cormack: The organisation – or the constituency tends to be the term that is used in FIRST – may be a single company, it may be customers of a network like ours, it may be users of the product. Cisco have a CERT for users of Cisco products so they have even less

control over what their users do, but if their users do not respond to a vulnerability Cisco is one of the major providers of equipment that makes the Internet work so there is a strong incentive for Cisco to try and make sure that their customers do respond to warnings, respond to events and incidents, even though they have no formal ability to say “do this” at all. There is a lot of variation, therefore, in the amount of control you have and the amount of visibility you have. We would contact a security contact at each university and say “We have had a report, it looks like this sort of incident, please can you fix it?”

Q60 Lord Mawson: I am just trying to understand exactly how JANET works; is JANET connected in a diagram a bit like petals so that you control the core bit and then there are different petals connected to it? Is that how it looks?

Mr Cormack: I think you have seen one of our network diagrams by that description. We actually control the petals in that we have 13 or 14 regional networks that, under contract to us, deliver service to our customers who actually do not connect to the core network that we run, so those are the petals. Contractually therefore we control them. The universities and colleges will then connect off those petal networks.

Q61 Lord Mawson: My experience of IT networks is that the technology is one thing but the personal relationships are really, really important.

Mr Cormack: Yes.

Q62 Lord Mawson: It is just a tool and I am just wondering how you facilitate the coming together of the key people so that actually the human interaction is happening as well as the technology?

Mr Cormack: Down to customer sites, when a site connects to JANET they are required to provide a number of contacts; one of them is the security contact and it can be a role, it does

not have to be a single individual, though we like to know the names of the people who do it precisely because it is a human interaction, it is not an interaction between roles or mailboxes or whatever. We run various events where we get to know them; I was up in Glasgow running a training course yesterday with people who are site security contacts, so we try to get to know them so that if we phone up and say “You have a problem at your site” they recognise our voice. It is very simple, they know it is JANET CERT phoning and not somebody trying to make them do something stupid. That is part of the establishment of a trust, a recognition, so that we can immediately get on to actually fixing the problem rather than going through some of the bureaucratic process that was mentioned which is who are you, what authority do you have. It also works on the international level. One of the things that really impressed the UK Government when they started getting involved within the international CERT community, there was an incident where machines on JANET and on DFN, the German research network, were attacking the university in Bosnia with a level of traffic that took Bosnia off the internet. Because the Bosnian traffic was routed through Slovenia it was causing Slovenia considerable distress as well. The head of the Slovenian CERT – I think they were members of FIRST at the time; we certainly knew we had met them – could just get on the phone to me as the head of JANET CERT and the head of DFN CERT and say “There is no legitimate traffic from your network coming to the University of Tuzla”. I could phone my network operations team and say “Please block all traffic from us to that address” and the attack was stopped within five minutes. That is the sort of thing that a bureaucratic process really just cannot do in that timescale.

Q63 Lord Richard: You are in effect an academic CERT to a certain extent and you are a banking CERT.

Mr Gibson: I am.

Q64 Lord Richard: But they are teams as I understand; how many have you got in each team?

Mr Cormack: In ours for the network we have nine posts at the moment.

Q65 Lord Richard: That is in the CERT.

Mr Cormack: Yes.

Mr Gibson: We have a model where we have a team of seven or eight people in New York who essentially manage incidents and they are the central point, all incidents are reported to them. They can then call out – they have a daily call, we go through all of the incidents that have come in in the last 24 hours. If they are of a certain severity then we will be on a call within an hour or two hours or three hours – as soon as it is reported we will take a view like this one is serious, we need to do something now, otherwise they are reviewed daily. We can invite people onto that call, the subject matter experts internally, so if it is a network issue we will call in the network folks, so the core team is about seven or eight people in New York.

Q66 Lord Richard: How many here?

Mr Gibson: I am part of that team as a subject matter expert for forensics, but the official team is seven or eight people in New York. They are on 24-hour call, we can get them day or night, but we have always tried to do that so that we have got one place that we know where everything is going on. We have had incidents in the past where something has been reported up this chain, it will hop through senior management and come down the line in New York. They wanted to know what was going on and the right people had not actually been informed at that moment, so we spent a great deal of time mandating this – you know, we wanted to go into one central point in New York, that 24 by 7 group you can call them day or night on their mobile phones and they will immediately react. If that means escalating it or actually taking action, that is not a problem, it happens.

Q67 Lord Richard: I am just trying to see how it works. Something happens at a bank in Britain, whatever it is, and that starts alarm bells ringing. It then goes to New York and it comes back from New York to you.

Mr Gibson: Depending on the issue. As I say, I do the computer forensics, that is what my team does for the bank. If it is a networking issue they may call out to someone else in London but from New York the folks there can essentially call the right people and get the right things done anyway. If it means taking a computer off the air and literally disconnecting it from the network electronically, they can do that from New York anyway.

Q68 Lord Richard: Is that the same with JANET? You have not got people in New York, I understand that, but is there some central body which then passes it back down?

Mr Cormack: Not really because our equivalent to Chris's countries or banks are universities and colleges so we have a central team of eight or nine people in Oxfordshire who will function like Chris's team in New York. One other difference is that I guess you have mandatory reporting.

Mr Gibson: Absolutely.

Mr Cormack: Any member of staff in a bank who discovers a problem must report it to the bank CERT whereas in JANET we exist as a service to the community. If the community wants help, if any member of the constituency wants help, they can come to us. So we have no mandatory reporting, but some universities may have their own internal teams. I should say that a team does not have to be as big as that, it can be very effective. A CERT is a process and needs enough people to run that process according to its desired service level, so there are some universities who will have one fulltime CERT person and two or three others, and part of their job is to help there, and they can be highly effective. Those would be sort of equivalent to Chris's branches and we would pass on reports to the relevant customer organisation.

Q69 Lord Mawson: My second question is why can CERTs be trusted and should the Government be getting involved to make sure they stay trusted? Is not the danger that this is a lot about relationships and is there not a real danger that the Government will try to turn it into the usual systems and processes which are absolutely alien to what a network is and they will frankly undermine what this is all about? Is there not a real tension here?

Mr Cormack: There is a tension but I do not think it necessarily is a bad idea. There are three ways in which trust is established. You mentioned person to person which is probably the foundation of everything. More recently there have been two different ways of establishing organisational trust; one is by simple declaration – JANET CERT is the CERT for JANET says the network operator, or CERT/FI is the CERT for Finland says the Finnish equivalent of Ofcom, so there is a sort of declarational, this is the responsible body. The third one I think of as expectation of delivery, so if somebody pops up and says “Hello, I am the CERT for such-and-such a network or country”, if I have an incident with them that does not involve too much private information on my side I will send it to them. If having sent it to them does not make things worse and makes things a bit better then I may send them more and you slowly build up something according to my expectations of what a CERT does. That is another way that it can be established. In the past three or four years there have been some attempts to codify that into best practice and there is a CERT maturity model being worked on which looks at relationships, funding, technical skills and position in the organisation is the fourth, so there are attempts to formalise “We are a CERT, we are capable of behaving like a CERT”. I glad you said Government coming in and messing things up so I do not have to. That could happen; however, we have a feeling for the number of internet addresses in Europe and the proportion of those that are covered by a CERT – or ISPs tend to have things that they call abuse teams which are more used to handling bulk incidents – is still only about 25 per cent of European IP addresses that have a CERT or an abuse team sitting somewhere above them.

There is, therefore, definitely a role for Government, European bodies, anyone, please, to try and help fill in those blanks on the map, the 75 per cent of IP addresses which, when I get an incident from them, I can do nothing about because I have no trusted contact. I am trying to encourage the UK Government to use the phrase “CERT of last resort” which does not sound as grand as national CERT but if you cannot find anybody else in the UK, ask us. There is a definite role there; there is a role in encouraging other sectors to develop their own teams, there is a role in putting teams together, there are organisational roles but there is less in an operational role because, as you say, it is a third party in a communication that maybe does not need to be there and may impose more bureaucracy than is needed.

Mr Gibson: We would very much like to see governments pushing “You should have a CERT” both for ISPs and for organisations because they are extremely valuable. Whether they get involved in the communications with them is another question but we would very much like to see more CERTs.

Q70 Baroness Garden of Frognal: Just following on from Lord Mawson’s question is there any sort of person specification for the individuals who work in CERTs and is there any vetting procedure?

Mr Gibson: To join FIRST, for instance, for a team to join they have to provide various pieces of information. They have to be sponsored by two existing members, there is a site visit, there is a document to go through where they look at terms of reference, is this genuinely a CERT, does it have a charter from its organisation to do the right things or is it one person pretending to do something they cannot, so it is very much sponsoring – do you know these people, do you trust them to join the organisation?

Q71 Baroness Garden of Frognal: Is that knowing the individuals or knowing the organisation?

Mr Gibson: Both I would say. There is a site visit, one of the two sponsors should visit the site and talk with the people and get to know them, and by sponsoring them they are essentially saying to the rest of the organisation “I know these people, they are good people, they should be members of FIRST”, so very much so. As FIRST has grown bigger and bigger that has become somewhat harder. Back in the old days there were 16 members, everybody knew everybody, you all knew each other by your first names and life was very easy; on the other hand you were only 16 teams and covering a tiny percentage of the Internet. Now we are 200 plus teams, we are covering a bigger proportion but that level of personal trust is harder because you do not know everybody. That is one of the reasons why we put on regional and global meetings every year, to get people together, to get them talking, to present, to learn about each other and to meet each other but that personal trust is harder and you have to work at it, but it is certainly doable.

Q72 Lord Hannay of Chiswick: Following up the same line of questioning is there even a theoretical possibility that a CERT could be taken over or established for criminal purposes and that this would escape the notice of other CERTs? If so, what would be the possible implications of that?

Mr Cormack: I think it would be detected fairly quickly by my test of when I send them information does it do good or does it do harm? They would have to make sure that they were visibly still doing good while covertly doing harm elsewhere.

Q73 Lord Hannay of Chiswick: My assumption would be that if they were a successful criminal organisation they would obviously have a cover, i.e. they would do some good in order to prevent you immediately discovering that they were there for negative purposes. I just wonder whether you could explore this thought because it is relevant to the issue about whether governments should be in any way involved at any stage because clearly it is

governments who basically take legal action against people who transgress within their jurisdiction.

Mr Gibson: I should have added actually that when the two sponsoring teams put the membership forward for a new team it is then sent to our entire membership who effectively have the ability to blackball that applying team. It has rarely happened, I can think of only one case recently that I am aware of and certainly should someone start suspecting a team that would very soon become known. Some of our teams have very, very wide contacts and spend a great deal of time doing this, and if they sent something and action was not taken it would very swiftly become known. We have the ability to revoke their membership, certainly, but it has not happened to my knowledge. Given that CERT teams are reactive, if they do not react then you take a view on why they are not reacting. If that is because you believe they are doing something nefarious that would soon become known and they would essentially be blackballed through the network. One other point is that FIRST builds these personal relationships so if I have an incident I do not send it to the whole of FIRST, I will use the contacts I have made through FIRST to send it to the right people so bad teams would not be picking up information I was sending out so to speak because I probably would not be sending it to them. If I did send them something it would be specific to their network and if they did not fix it then I would start suspecting their motives and integrity.

Q74 Lord Harrison: Is there anything useful we can learn from the recent instance you pointed to where, in effect, a CERT was blackballed by the rest of the community?

Mr Cormack: There are confidentiality agreements.

Mr Gibson: Yes, as part of FIRST membership.

Mr Cormack: The issues that were raised were both over the past history of individuals involved in the team and that people were doing things in there outside their day job that were felt to raise questions. That has happened actually on a few occasions, that teams have got

informal suggestions that they might like to encourage their staff not to get involved in certain activities in the evenings, plus a feeling that they were not fully committed to making things better which is the formulation – there is an expectation that you will not do harm, you will actually do good, and for the team that was refused membership it was not a single veto, it was a general thing, quite a lot of people had concerns so it appeared in that case that the personal networks were working quite well.

Q75 Lord Hodgson of Aston Abbotts: We had an inquiry into money laundering and, during that, we received evidence that in certain cases law enforcement agencies were part of the problem not part of the solution. Has this issue arisen in your area, that is to say there are jurisdictions where perhaps there are activities which cut across your wish to keep the party clean?

Mr Cormack: Let me take it from the other end. If you are a customer of JANET CERT I hope that people who report to us know that things go to JANET CERT, they do not go to JANET the company. When I was running the CERT I told the chief executive of the company “That is not your business, that is confidential information.” There are other organisations in other countries that are members of FIRST where I would not have that certainty, I would expect that information I sent to the incident response team, Chris’s group of seven people, would also be coming to the attention of higher authorities within that organisation or within that company, just as a matter of corporate, national or regional culture.

Q76 Lord Richard: I am getting a bit lost, my Lord Chairman, and I hope you can put me back on the right track. You are the banking CERT and you are the academic CERT, you have talked to each other but how? Is there some sort of central organisation into which all the CERTs link in?

Mr Gibson: FIRST has a mailing list, it has various websites and you can talk in a number of ways, and we see that as part of our role, to facilitate those conversations, but I know Andrew because I have met him many times and if I need to talk to Andrew I will pick up the phone and talk to Andrew, there is no requirement for that to go via FIRST, FIRST has served its function in bringing us together and building that relationship.

Q77 Lord Richard: Each CERT in effect acts for its own organisation or business or whatever you call it.

Mr Gibson: Constituency.

Q78 Lord Richard: And acts independently from all the others unless you want to pick up the phone or send an email or whatever.

Mr Gibson: It would depend on the information. If we see something happening that we think is Andrew's systems attacking our systems type of thing, we may put that across the mailing list and say "We are being attacked, we are not sure from where, can anybody help us?" so we would use the FIRST network there, but if I have identified it as Andrew's ---

Q79 Lord Richard: There is no central clearing house.

Mr Gibson: No.

Q80 Lord Richard: Do you think there should be?

Mr Gibson: Some of the privacy issues would just cause nightmares. Some of the EU pieces where IP addresses would perhaps be considered personal information have always been an issue for us. Our banking CERT covers over 100 countries: trying to nail that down would be ghastly and trying to formalise that and sending it to a very global list may not be the right thing to do.

Q81 Lord Richard: But you have a clearing house in New York.

Mr Gibson: We have in New York, yes.

Q82 Lord Richard: And you are the clearing house for the academic community.

Mr Cormack: If they want to use us. There is also a distinction between personal contacts and organisational contacts because every team will have an official contact email and contact phone number and they will have some level of service on that, whether it is nine to five or 24/7. So I can either report something to Chris if it is a general enquiry of are you interested to know that – maybe our users have reported that they have emails trying to phish their credentials for Chris’s bank – or I can formally report it from my CERT to his CERT.

Q83 Chairman: Can I just come in here because is there not a problem which could arise because information about vulnerabilities could be shared and become available to undesirable people? Is it not the case that if Cisco pre-announces a problem so that CERTs can react there is a serious problem with that?

Mr Cormack: The general feeling is that the malicious people know about the problems already and in general our problem is not knowledge of vulnerabilities, it is getting people to act to fix them. Certainly Microsoft announce vulnerabilities on the second Tuesday of every month and it is widely understood that the day that that information is released a large number of people start trying to reverse engineer to work out what the vulnerability actually was, because all Microsoft will give you is “Here is the code you need to fix it” but it is possible to work it out from which programme that is changing, which routine within that programme, you can start drilling down to workout what the vulnerability actually was, and it seems pretty widely understood that that happens in the malicious community. The vendors are converging on the idea that there has been a lot of variation between them as to how they treat vulnerabilities, but they are coming towards the idea that actually there is no point publishing

information before there is a fix, that just frightens people, that they can do nothing about it, but once you can offer a practical way of fixing a problem then the balance of interest is in spreading that information as widely as possible. Microsoft have 200,000 on their mailing list for notification of alerts plus every Microsoft system by default will call in and say are there any updates and get that information out. Certainly Microsoft boxes run by malicious people will also go and fetch those updates but the balance of the world's good is now felt to be once you have a fix, get that information out as soon as possible. Until you have a fix you try and keep things as confidential as possible and what seems to happen is that as Chris described, building teams with the skills to look at a particular incident, there seems to be a process of building teams to look at a particular vulnerability if there is a vulnerability that affects multiple products. You might find a general vulnerability in a protocol and every system that implements that protocol is likely to have the vulnerability so you then need somebody to co-ordinate at what point do we decide that we have fixes for 50, 60, 75 per cent of them and the balance of interest is now to get those systems fixed even though that could increase the exposure to risk of the others for which fixes are not yet available. There are half a dozen teams worldwide, I think, who do that sort of co-ordination. JP/CERT do it in Japan, the Finnish CERT did a lot, CERT/CC in Pittsburgh – that is probably it.

Q84 Baroness Garden of Frognal: The EU communication envisages “National” CERTs which cover more than just public sector infrastructures. Do you see this as a valuable sort of institution to create and how does it compare with the UK's approach of multiple CERTs?

Mr Gibson: Andrew's phrase of a “CERT of last resort” covered that quite well. If I have an incident within my organisation in the UK realistically I need to co-ordinate that within my organisation and I may not want to talk to the UK one and multiple other national CERTs that may be involved because that is going to complicate matters. However, there is a problem here, there is no CERT team, who can I call? That is a very valuable idea, so I am all for

CERTs but I do not think it should be mandated that every incident I have within my organisation in the UK has to go through that CERT because that is just not going to work. Obviously there are regulatory reporting requirements and so on and so forth and if it is in a number of countries then I am reporting into multiple CERTs and just complicating everything. Obviously if we need the assistance we will call it and our regulatory requirements will require us possibly to report into the New York Fed and so on and so forth, but I cannot see the logic of reporting it to 26 different national CERTs because it happened to be in 26 countries.

Mr Cormack: There is also a very valuable role that is still being performed by CPNI as they are now, which is having meetings of UK CERTs. They have a UK CERTs group and there are a few FIRST member teams within the UK so they are getting those together in a room to discuss in a reasonably confidential forum new discoveries, new incidents, new ways of tackling incidents, ideas about co-ordination, creating that sort of trusted forum. CPNI now call them information exchanges and there are things in the States called ISACs which are somewhat similar – Information Sharing Advisory Centres – but the co-ordination of it is good. It is not about dealing with individual incidents, it is getting people to know each other, to share good practice, to share ideas, to bounce ideas off each other. It is very useful.

Q85 Baroness Garden of Frognal: You are focusing again on real meetings with real people going to places rather than virtual meetings.

Mr Cormack: I am getting less hung up about technology. There is an additional value once in a while to getting people together in a room but FIRST works pretty well when we meet once a year face to face and the communications in between do tend to reference back to the last time we met. The call may well be about an incident but it may well start with a “Do you remember the conference dinner in Kyoto?”

Mr Gibson: If I have an issue in a country where I do not know the team I may know someone in another team there who may know someone in that team, so you have that extended level of trust that you have from past encounters.

Q86 Lord Mawson: What you are saying is to emphasise the point that it is the building of networks and relationships, making it easier for people to meet as part of the process, so I presume the last thing you want is a facility on a remote island somewhere that is meant to be responsible for some of that.

Mr Cormack: I assume you have a particular remote island in mind. It is not that hard to get to, I go there once or twice a year as well. I do not think you have to meet very often and most of the work I guess it would be fair to say is done by electronic communications, in which case it does not matter where you are. The face to face stuff is getting to know people as people rather than as job titles.

Lord Mawson: Having built a network in my experience that face to face stuff as you describe it was really critical, not all the time but having those moments when people could come together and understand each other and then they used the tool of communication – it was that inter-relationship. Certainly when we began to develop the network we thought it was just the technology but we soon discovered that actually it was not.

Q87 Lord Hodgson of Aston Abbotts: This is about systemic risk. The evidence we have received suggests that on the one hand we should pull it all together and try and guard the whole thing or on the other push it all apart and make it safer that way. Could you give us your views on that and also in that sense whether botnets or a natural disaster or a cyber-war attack could bring down the Internet, or does the present diverse structure mean that it is safe from that sort of destructive, systemic difficulty?

Mr Cormack: I am not sure what bringing down the Internet would look like. Certainly I would be confident that a botnet could take any university off our network. I did a back of an envelope calculation on sizes of attack a couple of years ago and came to the conclusion that by the time a botnet was big enough to break JANET's external connections then the networks that were bringing traffic to us would have their own problems that they would be motivated to fix. I am pretty sure you could take off a single organisation, possibly a single class of organisation if they were too tightly coupled, if there was too much of a central point. The Internet is such a diverse network or networks that I do not know. More likely – I was watching the news this morning and watching pictures of the flooding in Cumbria; there was a little throwaway line about that bridge that is going to have to be taken down contains communication cables and I thought ah, does that include ours? I cannot remember and I have not checked back to base. In fact the way our network works – the petals that were described earlier – it does not matter, traffic will go the other way round. The backbone infrastructure is designed to be completely tolerant and completely invisible of a single break, there is always a second route. Two breaks, choosing a bad point, will cause problems. I have not been directly involved in any of the attacks on countries that have taken place but my understanding is that they have focused on high profile systems organisations within the countries so if there is a single government website you take that down. Whether you take down a national broadcaster I do not know because if you are trying to have a high impact attack, actually the thing that is telling people that there is a high impact attack is one of your tools so it is trying to understand the motivation. I suspect I would leave the BBC website where it was.

Mr Gibson: I do not think we have seen in the past – 9/11 for example when the network interconnections in New York were taken down it did not bring the Internet down. It slowed it down but obviously there was a great deal more interest and a great deal more traffic, but

that did not bring the network down and I have not seen anything that tells me the Internet will collapse. Bits of it possibly.

Mr Cormack: That turned out to be two of my badly chosen cuts because it turned out that our main link went one side of the World Trade Centre site and the back-up link went the other side, but we had a link to New Jersey as well.

Mr Gibson: In my bank we build the network to cater for that, we will have satellite connections that are wholly separate from the ground connections until they get to the building so if someone takes a JCB and drives through it, fine, we have a satellite connection and it will work. It is a design issue.

Chairman: Let us move on. Lord Richard.

Q88 Lord Richard: My Lord Chairman, before I actually ask this question I have been gnawing away at the construction of these things so I wonder if I could just ask FIRST one or two questions about that. FIRST is a forum as I understand it, is that right?

Mr Gibson: Yes.

Q89 Lord Richard: How many members of the forum are there?

Mr Gibson: We have about 205 teams and 20 or so liaison members such as our group.

Q90 Lord Richard: How often do you meet?

Mr Gibson: We have an annual conference and that is a global conference – this year it is in Miami, last year was in Kyoto in Japan. We typically have about 450 attendees to that and in the regions that we are holding the global meeting we will have regional meetings, so in January we have a meeting in Hamburg.

Q91 Lord Richard: What sort of agenda do you have?

Mr Gibson: It is very much driven by the members. We have a call for papers, people put up things that they want to talk about, the programme chair will go out and get people to talk, so there are talks about things that people have done, things that people are doing, the latest tricks and tips on how to handle incidents, legal issues may come up.

Q92 Lord Richard: How big is the organisation's centre?

Mr Gibson: It is purely a volunteer organisation.

Q93 Lord Richard: But how big is it?

Mr Gibson: There is a secretariat, the people who arrange the meetings and do some of the hard work, four or five people, but it is very much a volunteer network. None of us get paid to do it. There are ten people on the board or the steering committee who try to co-ordinate things.

Q94 Lord Richard: Are they elected by the members?

Mr Gibson: They are elected by the members, five every year – they have to serve a two-year term. It is very much a members do – if you put in you will get out. If you choose not to attend the meetings and if you choose not to make yourself known you will not get a great deal out of FIRST. If you get to the meetings, liaise and put information into the mailing list and so on you will get a great deal out of FIRST.

Q95 Lord Richard: What is the spread of the teams that come there geographically.

Mr Gibson: Right now it is approximately 40 per cent North America, I would say 20 per cent Europe, 20 per cent Asia-Pacific. Africa is the hole on the map at the moment; we have two or three teams in Africa and we are very much pushing to move into Africa – especially due to the enhanced Internet connections that are going into Africa we are very concerned. Up until now their connectivity has been so bad that they could not really do any harm. Now

they are putting very large Internet connections into Kenya and Tanzania and various places; we very much want to push into there and we are looking at holding one of our regional meetings in Africa next year.

Mr Cormack: And South America.

Mr Gibson: We have South America too.

Lord Richard: Can I ask the question now that I was supposed to be asking?

Chairman: Before you do Lord Hannay wanted to come in at this point.

Q96 Lord Hannay of Chiswick: I just wanted to follow that up by asking whether in your experience you think that people at the top level of government or business or the military actually understand all this.

Mr Gibson: That has been a bone of contention within FIRST for many years. In fact we started an offshoot called the CEP – Corporate Executive Programme – because some of our members are very senior. We have got some people who have been very senior within various telecoms and so on and they recognised that they would walk into boardrooms and say “You are a member of FIRST” and the board would look at them blankly and say “What?” Most boards would understand that they had someone somewhere buried in a dark cupboard, looking at computers and keeping the place safe, but they did not understand that FIRST existed and that FIRST was doing all this good work and all the rest of it and thereby these teams may not be getting the resources that they need and the ability to travel to the conference and so on. We therefore started this group as a means of bringing more senior people into the mix, to learn both ways really, for them to learn that there is a group out there doing this and that they are part of it and also to get their take on the risks. Obviously most of our teams sit in bunkers and look at computers and field attacks and so on and they may not see the bigger picture from the board level and vice versa, so we wanted very much to set up this group to allow that interchange to take place.

Mr Cormack: I was going to move on to the government side. One of the things that has been seen by the community as very positive is the establishment and involvement of ENISA as an indication that it is seen as an issue. ENISA cannot join FIRST because it is not an operational body and as I understand it has no desire to be so, but there was a very strong welcome given to the members of ENISA staff who, like me, are now personal members of FIRST, so they are very much involved there.

Q97 Lord Richard: I suppose the question I am going to ask you is really a reflection of whether you think yourselves successful or not: how safe is the Internet for consumers?

Mr Gibson: If you practise the right things. Would I go and use a computer in an airport lounge to do my Internet banking? I do not think so. Would I use my home computer to do so, yes, so as long as you are cautious and careful in what you do – I do my Internet banking on-line, I do various things on-line, I am quite comfortable with doing that, so I do not see an issue with that. Some people take a more paranoid view, some people do not, but I certainly would not use any old computer that I happened to bump into to do it. Experience has taught us that a lot of the customer incidents we get in the bank are on such systems, so I think so, yes. I would not say that the sky is falling, do not use the Internet.

Mr Cormack: How a user behaves significantly affects their safety in the same way as how a driver behaves or a pedestrian behaves affects their safety. I am pretty confident that my parents are safe Internet users – they do email, they exchange information with us, they are not technically savvy at all – they may be watching. I would not regard them as technically skilled in the way that some of your witnesses may be but it is possible for the average citizen, exercising appropriate caution, to conduct their business safely on-line.

Q98 Lord Richard: Pretty confident does not sound too confident.

Mr Cormack: Accidents happen. There are reckless drivers on the Internet who put other people at risk in the same way as there are reckless drivers as I walk across Parliament Square.

Q99 Lord Hannay of Chiswick: In the EU paper we are looking at – which you are presumably familiar with – one of the suggestions is that there should be pan-European exercises carried out on large-scale network security incidents. Are you aware whether these exercises have ever taken place and have you participated in them yourselves? Do you think they are useful?

Mr Cormack: They certainly have taken place. Some European countries have been involved in American-based exercises; my only involvement has been, again, one of these face to face meetings where some ideas about a scenario were being bounced around and they were in an area where I had more technical knowledge than the others present so I was able to feed in some information which I hope made the exercise more accurate, more realistic. There was certainly a large one in the Asia-Pacific region as part of the preparations for Beijing which was co-ordinated by the Chinese CERT and they have been doing useful presentations on the outcomes of that that they found very useful, both in discovering hidden assumptions. You assume that a certain person will always be available, or you will be able to get at the FIRST website to get the encryption keys of the people you want to talk to and an exercise is much the best place to discover that those assumptions are not correct. The other thing is that it is another part of the building knowledge of other teams' understanding and having those contacts. Again, it is a point you can refer back to. We have not spoken since the exercise but I have not had a real incident so again you are straight into operational mode, trusting mode within 30 seconds of the conversation.

Mr Gibson: Again, FIRST is not an operational group so FIRST does the communications but FIRST as an organisation has not been involved although a number of our teams have. In my

day job for the bank, yes, we have been involved in some of the American cyber-storms as they call them, exercises where similar sorts of things are done and they have proved very useful. I would certainly say, yes, they are a good thing.

Q100 Lord Hannay of Chiswick: If you were to hear that the EU idea had been taken up and that they were going to carry out a big exercise like this you would not recoil in horror and think it was a waste of time?

Mr Gibson: No.

Q101 Lord Hannay of Chiswick: You would actually think it was quite useful and that it would extend and deepen your own knowledge.

Mr Gibson: Exactly, yes.

Q102 Lord Hannay of Chiswick: You have mentioned a little bit about ENISA and that you yourself go there a couple of times a year. Of course it is one of the areas we are looking at; could you just say what your impression of it as an organisation is and whether they are really able to deliver what the objectives of their programme set out, whether they are well staffed, and well situated geographically et cetera et cetera. Do they have the right powers and mandate to enable them to deliver the objectives that have been set for them?

Mr Cormack: One of the issues is that the objectives have changed significantly in the last year or so because, as I said, I have been involved in the stakeholders group for five years and for the first four of those years the words “network resilience” were banned, we were not allowed to discuss network resilience because that was a third pillar issue which was for Member States. They were resourced and their programme set up to exclude network resilience; they have now been instructed to make it a major focus so there is a challenge to work out whether they need to redeploy resources they have got. They are a very small

European agency; I suspect there are some corporate and national CERT teams that are bigger in staffing than ENISA so it is a small organisation. The timescales that partly the stakeholders group was involved in setting on the programme I hope are realistic. The paper, however, seems to set quite an aggressive timescale in that everything could be done by 2010. With their current resources I suspect they would struggle to do that but the skills they have would certainly enable them to do that, and the relationships they have with communities. Again it is this building up trust thing; they have spent five years going from most people in the community being scared that this was going to be an attempt to impose an operational organisation on top to actually discovering that they are really good at gathering good practice and identifying good practice, getting it written up and then disseminating it. I was mentioning to Chris earlier they have a guide to setting up a CERT which is now available in all the national European languages and Russian and they are working on further translations for extending areas. They have run exercises and training courses across the extreme points – in Dublin and Vilnius, I cannot think of the North to South but essentially covering the whole continent and beyond where people have particular interests. The Polish team have worked very closely with them on running exercises and training in the former Soviet republics, within any community referred to as the Silk Road area. That had immediate operational benefits when there were the cyber-attacks in that area, that suddenly there is a CERT, it has a basic set of skills, it is known. That is almost entirely through ENISA's work, I do not think that would have happened otherwise.

Mr Gibson: ENISA had the mandate to do the training throughout the EU; FIRST took that training material and then has given that training around the world as well – we have done it in Tanzania a number of years ago, we do it at our conferences, it is essentially a three-day course on how to set up and run a CERT team. It is classroom-based training that we have

done around the world, using the material designed through ENISA where they did not have the mandate to go outside Europe to do so.

Q103 Lord Hannay of Chiswick: So in what they do they are skilful and professionally good?

Mr Gibson: Yes, and they certainly made a very big effort to get out and to make the relationships with people that we have talked about. They have done that many times, they have come to conferences, they have joined as individual members.

Q104 Lord Hannay of Chiswick: Could you just comment on this question of the geographical location which comes up all the time and usually causes a good deal of merriment when it does come up. To what extent is it just a distraction in this particular field, or is it a real problem?

Mr Cormack: In this field in particular it is a distraction. The relevant staff are extremely well-known in the community, they come to meetings. They run an annual summer school which is a mix of academic and practitioner presentations in Crete which is actually a very good place to run a week-long conference, if you can get it past your finance people – “I really am going to work”. Most of the CERT work is done by electronic communication so it does not matter, it can be done on the train, it cannot yet be done on an aeroplane, and in some airports.

Q105 Lord Harrison: My Lord Chairman, it has been a fascinating morning and I wonder whether we might invite our witnesses to give advice to the Committee about the thoughts that we will come to put in our report. One of the questions we have to ask is whether there is added value in this European Union connection and some of the proposals that have arisen in the Communication. Listening to the two of you, you are clearly engaged in a network that is

successful partly or mostly because of personal connections but you have a fear of any imposed bureaucracy that might arise from the EU level. In so far as you learn information and indeed, as in your case, you impart information to those who perhaps need to know and be better acquainted with some of the pitfalls, what are your final views on the question of the added value of what is proposed here?

Mr Cormack: If I am feeling optimistic I can read the communication as very positive in supporting and extending the existing networks. I do not think there is anything in there that automatically gives me nightmares but as with many communications from governments it can be read in many ways so it may be a trite to say the devil is in the detail. It is positive that the Commission recognise it as an area that needs action, needs help. I think the Commission also appreciate that there is an existing, thriving, pretty successful community covering 25 per cent of the European Internet and I hope that they will see that as a model that they can follow to try and extend it to the missing 75 per cent and to increase the capability of what already exists. On the other hand it could be trying to impose on Europe something that is actually worse than the sort of thing that we tried in the late Nineties because the European CERT that we ran then was still voluntary, it was if you want to send incidents to us please do. The nightmare scenario would be an operational by mandate body that imposed itself at the top of the tree.

Q106 Lord Harrison: A recommendation would be that we use the successful 25 per cent to pass on as a model for the remaining 75 per cent.

Mr Cormack: Yes.

Q107 Lord Harrison: That certainly has utility.

Mr Gibson: Yes, and to use that European base as a kick start incident response team, absolutely.

Mr Cormack: While not being parochial – can you be parochial about something as big as Europe – and being willing to learn lessons from other areas of the world where they have had slightly different priorities and they have had different starting points. Asia-Pacific is different because largely they started with a completely blank slate, there were very few CERTs in Asia-Pacific until five or six years ago at which point governments and APEC-TEL stated that every country shall have a CERT by the time we meet next year. They came and looked at the rest of the world and said “How can we train these people?” and we said “Here is training material, here are trainers.”

Mr Gibson: Here are conferences, here are meetings, come and join them.

Mr Cormack: We took the conference to that area twice in that period, to Singapore and to Kyoto. We are willing, happy and interested to learn how others use the material that we use; we get a lot of good feedback from South America on the use of the European training materials that we will then try and incorporate. It works really nicely because of the shared languages – Spain and Portugal work is a very good channel to Latin America.

Lord Harrison: That is very interesting; thank you very much.

Chairman: Thank you, that brings us to the end of our session and we are most grateful to you. May I remind you of what I said to you at the beginning, that if afterwards you want to clarify or amplify any point please do so. I would also say, thinking of one question you were asked earlier on which I guess you were somewhat reluctant to answer fully, that we would be very content if you were to supply answers to that particular question on a confidential basis and we would give an undertaking that we would neither publish nor quote from it, but it would be helpful from a background point of you. To both of you, you have been very frank and very clear and we have had a really interesting morning. We are all extremely grateful to you, thank you very much.