Joint Committee on the National Security Strategy

Oral evidence: Cyber Security: Critical National Infrastructure

Monday 12 March 2018

4.20 pm

Members present: Margaret Beckett (The Chair); Lord Campbell of Pittenweem; Mr Dominic Grieve; Lord Hamilton of Epsom; Lord Harris of Haringey; Baroness Healy of Primrose Hill; Dan Jarvis; Lord King of Bridgwater; Baroness Lane-Fox of Soho; Theresa Villiers.

Evidence Session No. 1 Heard in Private Questions 1 – 25

Witnesses

I: Phil Sheppard, Director, Gas Transmission Owner, National Grid; Peter Gibbons, Chief Security Officer, Network Rail; Rob Shaw, Deputy CEO, NHS Digital.

Examination of witnesses

Phil Sheppard, Peter Gibbons and Rob Shaw.

Q1 **The Chair:** I thank the witnesses very much indeed for coming. We very much appreciate it. You were kind enough to say that that you would give evidence first in private so that you could perhaps be a little more frank with us than you might wish to be in public session. What will very much interest the Committee is the whole issue of resilience, business continuity and so on, and the nature of the threats that you face and how you are tackling them.

Perhaps each of you could begin by telling us what a worst-case scenario would look like for your particular sector.

Phil Sheppard: I am from National Grid. The worst-case scenario would be similar to what occurred in Ukraine in 2016: the interruption of supplies to consumers, time to recover, and a series of blackouts.

Peter Gibbons: I am from Network Rail. For us, the worst-case scenario would be a multiple train crash caused by interruption of the signalling

system or potentially a failure of the electrification supply system causing all the trains to come to a dead halt.

Rob Shaw: I am from NHS Digital. The worst-case scenario would be a direct impact on patient care, or adverse care as a result of an IT failure.

Q2 **The Chair: ***.**

Phil Sheppard: ***

Lord Harris of Haringey: What do you describe as a threat actor?

Phil Sheppard: It is an actor that has sufficient resources and capability to look like a state actor.

Baroness Lane-Fox of Soho: ***

Phil Sheppard: ***

Lord King of Bridgwater: *** As a totally non-technical person, my understanding was that the really skilful people can make the attack look as though it is coming from somewhere else and is routing through a different route.

Phil Sheppard: There are various characteristics and, with the support of the UK Government, that is where we believe these attacks are coming from, disguised or otherwise.

Lord King of Bridgwater: Is it GCHQ that advises you on this?

Phil Sheppard: It is GCHQ, the Centre for Cyber Security and the Department of Department for Business, Energy and Industrial Strategy.

Q3 **Lord Hamilton of Epsom:** What about the possibility of what I have described as sleeper bugs: they put something into your system and they trigger it a year later?

Phil Sheppard: That is one of the key threats and use cases that came out of Ukraine. Some of the preparations that went into that attack started 18 months ahead of the event. We monitor all the activities inside our networks, ***.

Lord Hamilton of Epsom: To what degree do you go through satellites and into the airwaves? Do you have closed systems?

Phil Sheppard: *** we have control systems that operate the transmission grids for gas and electricity. We refer to those as having an air gap—there is a space between them and our enterprise system—so regardless of the communications media that we operate on, we have back-ups, alternatives, separate routeing; we have a whole range of defence to make sure that we keep the two systems separate and reduce the surface attack area, if you like, for the CNI systems.

Q4 **Lord King of Bridgwater:** I have two questions for all of you. Do any of you give contracts to Global Switch? If you do not know to whom I am

referring, this is a company that has been bought by China, and I see in the briefing that we have had that the Australian Ministry of Defence has already cancelled its contract with it. Do any of you have contracts with Global Switch?

Phil Sheppard: I am not aware that we do.

Peter Gibbons: I am not aware of that. I would have to respond in written evidence.

Lord King of Bridgwater: You have not had any advice coming down centrally about that.

Rob Shaw: Not in my area directly. The NHS is an absolute beast, as most people will know; it is not a single thing. I would love it if it was a single thing, but each local organisation has its own commercial agreements with third parties. If we can find out what that threat is, we can make sure that we put out an alert about that particular supplier, but we would expect that sort of thing to come down from the National Cyber Security Centre.

Q5 **Lord King of Bridgwater:** One bit of advice that we have had from one of the people who have given us information or evidence is to ensure "that the critical national infrastructure services are only ever accessed and delivered by security-cleared UK national personnel", and that that will reduce the risk. Do each of you think that you have got that applied?

Phil Sheppard: All the people who work on our control systems in the control centres and that support the CNI systems have security clearance.

Peter Gibbons: From a Network Rail perspective, all our staff are checked through the government vetting system, and all contractors who work for Network Rail are also checked.

Lord King of Bridgwater: Checked by whom?

Peter Gibbons: By the policing agency Disclosure Scotland against the basic personnel security standard, and those who are operating within secure systems with authority are vetted up to a high level of security vetting.

Rob Shaw: It is the same sort of thing for the NHS[1]. We have on-board vetting for all our permanent staff. We take up references before people start. That used to be a weakness when you wanted people in as quickly as possible, but now we make sure that we get the right people in. We also do Disclosure Scotland checks.

I was not sure if your question was about the people who are working within our organisations or the parent companies. Some of our companies that provide major IT systems—Cerner and Allscripts, for example—and others that provide a significant amount of the estate for hospital

[1] Witness correction: should read "NHS Digital" not "the NHS".

administration systems and electronic systems for hospitals,[2] are outside the UK, but the security of those is still managed within the estate of the NHS.

Lord Harris of Haringey: I want to follow up this question, because a very important point is being looked at here, particularly with regard to your data.

We have had a submission from a cloud provider, who has said basically, "It is all these big international cloud providers that tend to win the contracts, but we are in the UK and we'd be suitable". That is their pitch, but where your data is stored is an important issue. Presumably it is often stored by a cloud provider and often not by one that you own yourselves. Unless you have gone to exceptional lengths, you cannot guarantee the physical location of the server; where they are actually storing the data.

Peter Gibbons: All National Rail's critical national infrastructure systems are within our control. We own them. We operate them. They are in our secure locations, typically rail operating centres or our own data centres. We have a cloud security policy that allows us to run through a risk assessment process every time we put data out in the cloud to make sure that the only data that goes out is not connected to a CNI facility.

Phil Sheppard: We have the same arrangements. We do not put our critical national infrastructure data into the cloud; we have data centres and other systems that keep that separate from the rest of the world.

Lord Hamilton of Epsom: So Network Rail has an air gap, effectively, so it does not go up into satellites at all?

Phil Sheppard: Correct.

Rob Shaw: At the moment, our network is provided by BT and we are transitioning to what we call HSCN, which is breaking up that network. For the large contracts, of over £100 million, we have looked at different ways of sourcing those services. They are all managed onshore and we have not put any of our critical national infrastructure, such as the Spine, into the cloud; that is all on frame at a secure data centre. It is not a single data centre; it is in two locations so that we can failover and failback, which we rehearse regularly.

The other side is that we have a cloud policy, and it sounds very similar to Peter's: we do a risk assessment that has to be signed off at SIRO or CIO level. There are strict limits on where you can and cannot store identifiers or personal confidential data. We do not store anywhere outside the EEA. Within the EEA, there are only certain countries in which we will allow data to be stored. Again, that is a policy that we have put out to the NHS for it to use as a standard.

---

[2] Witness correction: "electronic systems for hospitals" should read "electronic patient record systems".

Q6 **Lord Campbell of Pittenweem:** Have you ever found any of these bugs—I call them bugs, forgive my ignorance—or sleeping techniques when you have conducted searches of the kind you have described?

Phil Sheppard: We have found nothing directly relatable to what happened in Ukraine. One of the processes that we have, though, is stopping a lot of those entering the system in the first place.

Lord Campbell of Pittenweem: Have you ever found anything that broke into the system? If so, what?

Phil Sheppard: That is a simplistic way of looking at things.

Lord Campbell of Pittenweem: Well, I am a rather simple person.

Phil Sheppard: I am sorry, forgive me. It goes back to having a perimeter, and once something is inside the perimeter it is passed through. These days we think of it as defence in depth. If, for example, someone takes a laptop off our estate, logs on, goes to a malicious website for some reason and brings it back on to our estate, we can immediately detect that they have gone somewhere they should not have gone, isolate that laptop and take it to our forensics laboratory, and then we can understand what has occurred.

Lord Campbell of Pittenweem: I am trying to get some sense of the extent to which you are or are not under siege. How often does the laptop situation you have just described occur?

Phil Sheppard: Not very often, because we have devices on the laptop and the laptop hard disks are encrypted, but the key thing for us is culture—making people aware of what they should and should not do. We do lots of phishing trials; every now and again we send people a malicious link to see if they click on it and then we send them to a training video. We do those sorts of things to try to improve the resilience of our people and to avoid people being socially engineered—being rung up and asked for details on the system. All those things are cultural, and they are very important to protect the physical assets.

Lord Campbell of Pittenweem: I do not doubt any of that. That is policy, no doubt, and administration. I want to know whether there are any penetrations. Are there any occasions on which any of you have said, "Something has gone badly wrong here"?

Phil Sheppard: For us, no, there has not been a situation in which things have gone badly wrong.

Peter Gibbons: From a Network Rail perspective, it depends on what you mean by "badly".

Lord Campbell of Pittenweem: Penetration of a capability that has the means of causing the diversion or destruction of your objectives.

Peter Gibbons: We have had two incidents of note in the past 24 months. One was a distributed denial of service attack, which greatly

reduced the capacity of our data centre. It did not impact on the running of our critical service—the movement of people and goods on the rail infrastructure—but it did cause us internal issues with staff productivity. We had a very, very small number of incidents—fewer than 10—of ransomware from the Petya bug, which followed WannaCry, which were dealt with in a space of hours.

Going back to Phil's earlier point about scale, it might be helpful to talk through some of the numbers that we experience at Network Rail. In the past 12 months, we have intercepted and blocked 288 million bad emails—emails with malicious content.

Lord Campbell of Pittenweem: Forgive me, what do you mean by "malicious content"?

Peter Gibbons: It either has a virus attached to it or some form of malicious active software embedded in it, or it has some content that we would not condone, such as sexist or racist material.

Lord Campbell of Pittenweem: Can you tell us the percentages of those three categories?

Peter Gibbons: We block around 89% of all the email we receive. So 11% of the email that Network Rail receives is legitimate. The rest is bad and blocked and never gets near our people.

In the past 12 months we have blocked 76 million web-based threats—attacks coming from websites that our people are looking at: that is, hostile content hosted on a website that our people have visited. We have blocked 1.6 million high-risk network attacks—these are the threat actors, people actively trying to have a go at Network Rail over the internet. We have stopped 19,000 viruses infecting our laptops and desktops. Some 440 of those viruses successfully infected a machine, so going back to your question about how many actually hit and caused a disruption, in the past 12 months we have had 440 virus infections.

Lord Campbell of Pittenweem: And the NHS?

Rob Shaw: The numbers are large, but when you put them against the amount of traffic that we receive, you tend to find that in both the public and private sectors the percentages of what does and does not get blocked are quite similar. In November alone we blocked 52 million harmful activities across the N3 network. That is a bit lower than average; we normally get between 55 million and 60 million malicious software activities per month. We have prevented 2,400 potentially harmful files being downloaded; people have looked to download the content and we have sandboxed them and stripped out the malicious content.

Sometimes that can be needed. For example, how do you define images when you work in the NHS? Some software will stop an image of a bare leg, but if you are a clinician and you want to see a leg you probably need to see a leg, so it is a bit more difficult to work out what is and is not to

be blocked. So we sandbox things. People look at them and if they are normal traffic they are allowed to go on.

We have seen 6,966 targeted notifications of infection, which, going back to your question, is about machines that look as though somebody is trying to get into them, and we send notifications out. We see what is happening at the perimeter and through something that we call enhanced threat detection we can say at a machine level, "This is trying to get on your machine", so that people can either take it off the network or speak to the user about what they are trying to access, et cetera. We have quite a high number, but when you put that against something like the Spine, the peak load of transactions is 3,200 per second, so it is about four times more than the number of credit card transactions in the country. So a huge amount of messages are hitting.

You asked earlier about what has got through. We have seen one or two things that have got through and that have been lying dormant on machines that were then picked up by scans. These come particularly from emails and fake emails. With the best will in the world, unfortunately not everyone wins the Nigerian lottery on a weekly basis, but it is one of the easiest phishing attacks that we still see. We have seen the same distributed denial of service attacks as Peter has, where people are trying with brute force to get through the front door.

On the critical national infrastructure point, that does not affect us at all. First, we can block quite easily and, secondly, if we need to we can fail across to a different site. Not all hospitals have that ability to cope at a local level, so that is normally when we get involved in an intervention. One hospital, whose chief executive said that they wanted other hospitals to learn from this, was being used *** to send out mail that looked as though it had come from the hospital. It was not directing people to an inappropriate site, it was using it for advertising, but the hospital did not realise that at 1 am a million emails were being sent from the hospital.

We were seeing a lot of suspicious traffic and we thought that was unusual. We were able to go in and work with the hospital. Everyone was focusing on the primary site, but people had forgotten that the secondary site that was used only in an emergency could still be accessed. That is where they found what you would almost call a backdoor method of being able to get through.

It was not impacting on patient care, but it looked legitimate. So if you got an email you would think it was legitimate because it had come from a legitimate email address and you would click on it. If it was a ransomware attack, you would have picked up some ransomware.

Q7 **Dominic Grieve MP:** This question applies to the three of you, but it was the answer to the first question on behalf of the Grid that provoked it. Has it been possible to deduce whether the attacks that you felt were sufficiently serious to look as if they might come from a state actor were for the purpose of accessing information or actually able to destroy your systems?

Phil Sheppard: I do not have the detail on that which I can share with you. I am not sure that we can provide that via written evidence either. You could perhaps ask the National Cyber Security Centre.

Dominic Grieve MP: Does the same apply to Network Rail?

Peter Gibbons: We have not attributed any attacks against our critical infrastructure to a foreign state.

Rob Shaw: For the avoidance of doubt, WannaCry was not an attack on the NHS, even though it was quite well reported as being such.

Dominic Grieve MP: No, it was generalised, I appreciate that.

Rob Shaw: *** The call as to whether or not an attack was by a state would come from the National Cyber Security Centre or GCHQ. All we would do is provide the information about the attack, and it would be down to them to find out. We can see things such as the kill switch and pass that information to them. It is not just that attack that the National Cyber Security Centre is seeing; it is the same sort of attack across different areas, so it pieces that together.

Q8 **Baroness Lane-Fox of Soho:** Building on that, how do you respond and how do you practise your response? Has that changed over the past year and a half?

Peter Gibbons: It has changed quite significantly. About three or four years ago, we started to have a more detailed conversation about cybersecurity with our board. As a result we have invested quite heavily in our controls.

Baroness Lane-Fox of Soho: What is "quite heavily"?

Peter Gibbons: £30 million over the past two financial years. We have introduced a security operating centre in Manchester with the technical facilities to monitor all the systems that are part of our critical infrastructure. We work with BAE Systems to develop an instant response process and a set of "playbooks"—the means to follow any type of incident through a set of steps and processes, initially to detect that we have been attacked or compromised, then to be able to respond effectively and report back to the appropriate agencies that we have been attacked or compromised, but then to contain that attack as far as we can so that we can recover the service quickly.

Baroness Lane-Fox of Soho: Do you simulate attacks? Do you practise?

Peter Gibbons: We do. Every two months we simulate one of those plays from the playbook. We run through it with each of our security teams to make sure that if we are attacked in a live situation they know exactly what to do. It is well rehearsed and they know how to respond.

We also work cross-sector through the DfT on cybersecurity exercises—in fact, there is one on Tuesday next week—where we get together with the

train operators and the National Cyber Security Centre and walk through a scenario to make sure that it would not be just Network Rail responding to the incident; there would be a response as a sector.

Phil Sheppard: National Grid is very similar. The investment curve is continuing.

Baroness Lane-Fox of Soho: Is it enough?

Phil Sheppard: Yes. Part of the debate is: how much do you not know? That is where we are very heavily reliant on government and the agencies to inform us of future threats and capabilities that we should be building. We use a "predict, prevent, detect and respond" model. The more we can predict, or others can predict on our behalf, what is going on, the more we can look at how to prevent those in the first place; then how we detect them, and then, if something does occur, how we respond—how we isolate that part of the network. We rehearse these quite regularly.

As I said, we do everything from cyber phishing of individuals in our organisation through to running exercises. We run industry-wide exercises through BEIS. We have very close relationships with the appropriate authorities, such as the Centre for the Protection of National Infrastructure. We even have secondments between some of these teams, so we have some of our people embedded at the National Cyber Security Centre and vice versa.

Rob Shaw: We do a number of different things to rehearse. We have business continuity planning. NHS Digital has set the scene that we are the trusted technical advisers for the system but we are not a regulator. We do not mandate. We work with those that have those regulatory powers. We sent a lessons-learned review post WannaCry to the Public Accounts Committee last month, which has more than 20 recommendations that the system needs to do better. It was a real wake-up call for the service. The NHS always responds well in a crisis. We now realise, and the service now realises, that cybersecurity is another threat that will need to be treated as an emergency. We now have that through the emergency preparedness response that NHS England has run through its regional teams.

On business continuity planning, hospitals, major trauma centres and ambulance units regularly run rehearsals, such as going back to paper. In a disaster, which we have seen a number of, unfortunately, in the past 12 to 18 months, no one worries about the IT system—you take somebody into the hospital, you treat the patient. The NHS needs to be able to continue to do that.

We are learning. The centre did not respond as quickly as it should have done to the WannaCry attack. There are a number of reasons for that, but one of the main issues—and what we learned—was that the runbook was ambiguous about the roles and responsibilities of who does what at

what time. It was clear who was involved, but decision-making becomes much harder in a pressured environment. So we have cleansed that.

It is now very clear who does what at what time. We have done desktop exercises with the NHS and all the central bodies about how they should respond. An example is the time at which you would declare emergency preparedness, because the second you start going into business continuity, that in itself has an impact on the way we deliver care to patients. You do not want to call it if it turns out to be a false alarm and you have a load of people not turning up to A&E and things like that. We have done a lot of work with local organisations. It has now got to board level.

All the discussions we have had so far have been about the technology. When it comes to preparedness for cyberattacks, it is as much about people, processes and culture as it is about technology. That is almost the last thing you need to worry about. If your people are not trained and you do not invest in your people so they understand it, with things such as the phishing exercises you can spend as much as you like.

*** So it is about where you spend the money wisely to be able to do enough, and then how prepared you are for when there is an attack, because there will be something that gets through the perimeter.

In the same way as my colleagues do, we do a number of simulation games. *** We put ourselves up against the private sector, and I was quite pleased because our team won when it came to spotting some of the incidents that had happened. If you do not challenge yourself and work with the supply chain, all of a sudden you are insular, and this is not an insular issue: it works across boundaries. It does not know country boundaries and it does not know public and private sector boundaries. If there is an attack on a network, it will cross all networks. So there is a fair chance that we will all face the same attack.

Q9 **Lord King of Bridgwater:** In the briefing you gave us, it says that 80 NHS organisations were hit by WannaCry because they had not applied the patch, but most of the NHS did. Was everybody notified of the intelligence of a specific threat? Was it just those 80 organisations that did not do anything about it? Was that because they did not understand, could not afford it, or what?

Rob Shaw: That is a good question in relation to the impact of that particular attack.

We sent out two broadcasts to all organisations, not just hospitals—so those 80 were 80 out of 240 hospitals. We send targeted mail out to everybody in the system who is impacted by a certain type of attack. WannaCry impacted everybody potentially, so we sent the mail to a list of all our security specialists and all our CIOs in the system. Those 80 were not all impacted directly by WannaCry.

Some of them took action as a result of the threat; they took themselves off the network or disconnected themselves from mail because they did

not really understand the threat. Part of their decision-making was, "If you come off the network and you're not affected, you can still treat patients". The impact of making a decision like that without working through the outcome of taking yourself off the network is that you are suddenly radio silent, and the question then is how we can get information to them and how they can get information back to us.

As a result, we have now had to set up a secure SMS service for people who take themselves off the network. All those 80 organisations received the patch and advice telling them what to do, and some of them had patched Windows XP et cetera, but they were still vulnerable because the firewalls were not secure on to the network.

******* overall the NHS, even including the 80 that were hit by that infection or that took steps, responded really quickly to get the service back and to keep the continuity.

So I do not think it was just a case of them not having not patched; a number of different reasons added up to the 80 not patching. But nobody who patched was impacted. That was one of the biggest lessons that we learned. We have now got to the point where, even though we are not a regulator, if we send out a high-severity alert, they must respond within a period of time to say not only that they have received it but what their plan is to implement that change.

We did not have that before; we assumed that when we sent an alert it was acted upon. One of the lessons that we have learned and one of the ways in which the NHS England and NHS Improvement team have helped is that they are now required to come back and say what activity they have taken, so we know that if there an area that has not patched, we can go and support them.

Q10 **Lord Hamilton of Epsom:** My question is also for Mr Shaw. The NHS has a plan to put everybody's medical records on to a computer base. Has that happened now, and is that a secure system that does not depend on the airwaves?

Rob Shaw: It has happened in some ways. You can get access if your GP provides access to your GP system at the moment. You have a right to see your records. You can see repeat prescriptions, et cetera, which makes it a lot easier for patients. You can also see when your bookings are on, and things like that. As part of our Personalised Health and Care 2020 programme, we are looking to put more online.

You can look at this in two ways. Before the NHS online programme goes live, it goes through our service acceptance criteria. The Secured by Design assurance process is the penetration test that things take before they go live, and it is significant, because this is a centrally provided service. You could say that you increase the threat vector by giving nearly 60 million people access to their own medical records, but you are only allowing them to see a copy of the record; you are not allowing them inside the application.

There is another way of looking at this. During WannaCry, if you turned up and the hospital system had been encrypted, if you had a record on your own smart device that showed that you had your own records, you could still be treated in an emergency. If you can access your own records when a single system goes down, it is in fact part of business continuity.

You could argue both ways, but because it is in my area before it goes into live service, nothing will go live to hit a date or a commitment until we know for a fact that it is completely secure as a service.

Lord Hamilton of Epsom: So that does not use satellite communications, then. It is all dependent on landlines.

Rob Shaw: It uses the internet in that you access your records through your device via a secure internet, but you can secure the internet as well in the way these records are accessed. It is not a case of, "We'll just put the whole of your care record on to the internet"; we will also allow different levels of access, depending on how you access things. We will not put personal data on that has a load of your clinical history in an area that has the same level of security that you need to access your demographic or to update your booking preferences or your opt-out of data sharing. We have a granular approach to what we are actually providing you with access to your record for, and it will have different levels of security, depending on how far down you go with that.

Q11 **Lord Harris of Haringey:** I have two questions, one specifically for Mr Sheppard. Last year, or maybe just at the end of the year before, the US Defense Science Board said that the US electricity grid was so effectively penetrated by the Russians and the Chinese that both states could, at will, switch off the electricity grid in the US.

I have asked here, and not got an answer, whether we think that our systems here are similarly penetrated, and I would be interested in whether or not, despite your earlier answer in which you said that you stopped a lot of stuff getting on, you feel that might be the case here. Then I have a more general question.

Phil Sheppard: That is not the case for Great Britain's national critical infrastructure, as far as I am aware. It is one of those known unknown-type things, but given all the work that we have done with government and the number of audits that we carry out—we even now check the supply chain and the components that go on to the transmission network to make sure that we understand where the firmware has come from and to see whether there is anything hidden inside the relays that get put on to the system—it is very unlikely that anything like that exists in the Great Britain network. And we work continuously to find other ways of testing that that is the case.

Lord Harris of Haringey: But as a company, more of the National Grid operates in the US than in the UK. Are you saying that your US counterpart, part of the same company, is less secure?

Phil Sheppard: No. We have the same relationship in the US as we do here with the FBI, the Department of Energy and the Department of Homeland Security. National Grid business in the US is a distribution business, not a transmission business; it does not have the same critical national infrastructure. But the work that we carry out in the cybersecurity aspects are identical, so we are as confident about our US assets as we are about our UK assets.

Q12 **Lord Harris of Haringey:** My general question is to all of you. I accept that this might not be your responsibility in your organisations, but do you look at the full range of your organisations' key suppliers, and what are your expectations of those key suppliers' cybersecurity? Clearly, your businesses would be just as disrupted if something absolutely vital to your operations, and which you cannot protect because it is provided by somebody else, stopped working?

Peter Gibbons: At Network Rail, we looked at all our tier-1 suppliers—those that are the largest chunk by financial spend—and ran through a cybersecurity health check with them to make sure that they are doing everything that we would expect them to do.

At the same time, we introduced a cybersecurity policy for procurement, so any new supplier contracts that are written go through a process to understand whether they are accessing our systems or our information or are providing products to us. If they are, they go through additional checks, and we require that they are either certified to the Cyber Essentials scheme or are ISO 27001-certified.

We make sure that they can demonstrate proficiency in cybersecurity before we go into the contract stage.

Phil Sheppard: Our procurement processes are very similar. Particularly because of the sensitivity of what we do, we are very careful who we partner with, and we make sure that their third-party suppliers and everything else go through the same process.

Rob Shaw: I would say that all three of us are in the same area. Anyone in our supply chain has to be ISO 27001-certified,[3] and we have an annual self-assessment that all suppliers delivering to the NHS have to look at. It has changed from the IG toolkit—the data security toolkit—in that the information that suppliers are now asked to provide is more meaningful.

The area that we keep an eye on, and we are providing guidance to the rest of the NHS to keep an eye on—this goes to your point—is the supply chain's supply chain. Verizon did a review in, I think, 2014 that showed that 90% of data breaches were in small organisations that were part of a supply chain. They were not the major suppliers. So we make sure that the responsibility of the prime supplier to check their own supply chain is regularly updated, and we have SLAs and penalties not only in relation to

[3] Witness correction: this should read "compliant" rather than "certified".

their providing that information; if there are any breaches they have to report to us, and that then goes through to the Information Commissioner.

Peter Gibbons: We do not see the challenge being our direct suppliers; it is our suppliers' suppliers, particularly when we buy a standard product off the shelf because we have less control. We would not sit down with Microsoft and tell it what our security policies were and what it had to write into its operating systems. That is where the challenge in the supply chain is at the moment

Q13 **The Chair:** I will ask you a really horrible question, to which I fully appreciate there may not be any possible answer. That is what you are all doing now because everybody is so much more aware of the supply-chain risks. Is it likely or possible that you still have vulnerabilities that come from a time when you did not do that—that there is stuff in your system?

Phil Sheppard: Yes, absolutely. One of the things we have established is an operational centre where we take new components and existing components that are on the network—protection relays and control relays that operate the network—and hack them. We work out what is in there, what the firmware is, and whether there are any loopholes that have been introduced either deliberately or inadvertently.

We work through the program to discover whether there is anything there we are not aware of, for exactly those reasons. Ten years ago we could upgrade something with a USB or a laptop, but now it is something that we spend a lot of time thinking carefully about—what process are we going to go through? If we allow somebody on our site, do we escort them, do we check the firmware, do we check the laptop, before we allow them access to our operational equipment?

Q14 **Theresa Villiers MP:** I would like to ask about medical records, to follow up the answers you gave before.

I have huge anxieties about the risks associated with millions of people having their records held in electronic form, potentially vulnerable to cyberattack. A key point is GPs. GPs are absolutely wonderful people who work incredibly hard, but they are really busy. They are often under pressure. They have lots to do. In many cases they are independent-minded, they are almost semi-detached from the big organisations of the NHS, yet they are part of NHS Digital.

What steps is the NHS taking to make sure that GPs install their patches? You spoke before about the need to ensure that people understand how to reduce cybersecurity risks and that it does not matter what technology you have; if the people in the organisation are not doing what they need to do to protect themselves from attack, the technology will not save them.

Particularly in relation to GPs, what steps are you taking to ensure that that kind of vulnerability within the NHS Digital systems does not lead to the disclosure of medical records?

Rob Shaw: I can give you some good news: it is not down to individual GPs. The software that is provided to GPs comes from four different companies, based in this country. Two dominant suppliers have 80% of the GP footprint. They provide the application. The GPs see the individual records of the patients as they come in. The GPs never have to patch their own machines, they never have to update the applications that are providing those systems. That is all done as a result of the contracts we have with our GP suppliers.

You are absolutely right that GPs and NHS workers overall are trusted to hold patient data. As we roll out new functionality—people said the same thing about banking 10 years ago: why can you not close down banks, and why can you not get money out of a hole in the wall and do internet banking?—a different set of pressures faces the NHS, but a lot of it has a similar sort of progress. You do not just do it overnight. The second we had a major breach, we would lose public trust, so people would not want their records online. So it is absolutely right that we make sure of that before we roll out at scale.

I think that around 11 million to 12 million people already have access to their GP records, because it suits them to be able to do things such as repeat prescriptions rather than having to visit the GP. They have access to those records, but we have not launched it as a great big central data store that is holding everybody's records somewhere. People can access that application, but the data is held securely in data centres that we have assured, in this country, on premises, so the risk with GPs is not as big as you would think. In fact, some GPs were impacted by WannaCry because they were connected on the network to a hospital, which then took itself off the system.

***

Theresa Villiers MP: Human nature being what it is, it is so difficult to remember never to click on an attachment. Even if GPs have their machines patched for them, it is easy to end up opening an email or clicking on a link that you should not. What is being done to address that specific risk?

Can you assure us that if a vulnerability got in through a GP's surgery, it would not affect a large amount of data? What steps do you take to ensure that where the worst happens and the bug gets in, the consequences, such as disclosing patients' data, are not significant?

Rob Shaw: I will take those two points separately. You are absolutely right that GPs are great people but, like everybody else, are also fallible. They will click on attachments and there will be things that they will put into their system, and there would be consequences if it was not protected from the outside.

We talked earlier about the number of threats and links that people will click on that get blocked now, and we go through whitelisting, et cetera. You can significantly reduce the risk of that, so you take some of the

human error out. The GP still needs to do the data-security training in the same way as everybody else, so we put them through that, even though they are busy people.

*** Because of the network vulnerability scanning that we do because of all the software that we have running on the machines, et cetera, you can see as soon as data starts to go to places it should not. As soon as we find out that that is happening, we can make sure that we can stop that, and we work with a number of big NCSC-accredited suppliers that we can call and they can deploy people on the ground quite quickly. The question, if that happened in an organisation that did not have those links or that capability to scan across, is whether or not they would spot it early enough.

Ciaran Martin, the director of the NCSC, has said there will be a category 1 incident in the next 12 months. He firmly believes that. We have to be ready to respond to it. We have the locking of the front door and trying to do everything we can to stop GPs getting infected, but we also have to make sure that if something does happen we have a culture in which people are not scared to report things. It is easy to beat everybody up and use the stick of saying what they should not do. I would love to get to where some of the energy companies and airlines are, where near misses are used for training so that people can think, "That has happened to me. I can learn from that". We need to build that culture in the NHS. I think we are getting there. Dame Fiona Caldicott has played a huge role in relation to openness and transparency.

There are 1.2 million people who work in the NHS. If we can train them to look after their IT properly, they will go home and help their children or other relatives with it, and they will keep themselves secure online. That is quite a big proportion of the population. We want to make sure that we normalise cyber. We need to get to the position where it is treated in the same way as any other threat is and we do not label it. As soon as you say "cyber", people get scared. They think it has an impact and that we cannot treat patients in the way we want to. If your bank account or your credit card is attacked, someone can spend money on it and you can work out your maximum limits. You cannot do that with healthcare. The smart review that we provided for the PAC talks about this: how we can make compliance with a lot of this a reality and help with carrots and giving out funding.

Martha asked earlier: what is enough money? We know the vulnerabilities in the NHS trusts, so when we are doing on-site assessments, telling them there are vulnerabilities is fine, but the NHS is strapped for cash—everybody knows that—so what do they do? They have to decide whether to put money into cyber rather than spend it on something else. We have put £21 million aside this year for hospitals to bid against to improve their protection. We have set £25 million aside next year for the same thing, so that the major trauma centres, foundation trusts and ambulance centres can to secure their hardware.

In addition, £150 million of funding in the spend programme has been reprioritised so that we can do more centrally to secure the perimeter. That seems like a lot of money, but it will protect all the NHS and into social care, because we will be able to get better advanced threat protection to know what is happening where. At the moment if you ask what hardware is deployed in a trust, you will be lucky if the CIO knows. It is a really complicated estate. If we can find out what is deployed in each organisation, we will know where all the vulnerabilities are. The NHS, the Department of Health and Ministers have decided that we should reprioritise some of our spend to make sure that things are secure before we continue with that spend.

Q15 **Lord Hamilton of Epsom:** When defence buffs are war-gaming the next big conflict, they think that the first thing that will happen is that the satellites will get taken out because so many defence guidance and navigation systems depend on them. Could you remain in business without any satellites?

Phil Sheppard: Yes. We use satellites as part of the internet. We recover information via satellites for some of our telemetry systems, but we have alternative routes that do not rely on satellites. Occasionally, satellites are affected by space weather and other things. We have defence in depth in that scenario.

Peter Gibbons: It is very similar for Network Rail. We use satellites for train location, but they are not our primary means of train location. We use the signalling system and track circuits for that. We would be okay.

Rob Shaw: We are not quite as advanced, but we are quite okay with that.

Q16 **Baroness Lane-Fox of Soho:** You have all mentioned the National Cyber Security Centre. I am interested in how you think that performs, how it helps you, or does not help you, and what more it or other agencies could do to help you.

Phil Sheppard: We have been building a relationship since it was established. It is going well. It is very supportive. As I said, we have had secondments between the organisations. One of the capabilities that we have is a secure platform that BEIS provides us with. For example, if one of the energy companies spots a bad domain, we can instantly share that among all the energy companies—gas, electric, distribution and transmission. That relationship works well.

Going forward, we are looking to get more intelligence as the threats and the capabilities grow. Some of the tools are becoming more commonly available to smaller parties on the internet. The more we can do to predict what is likely to happen and do scenario planning for that, the better. But I would characterise it as a good, strong relationship, and it is working well so far.

Peter Gibbons: From a Network Rail perspective, we have a good relationship with the NCSC and have had since its previous CPNI days.

We use a number of the tools that it provides under the Active Cyber Defence programme. We take advantage of the information exchanges and the CiSP information-sharing tools that it provides. We struggle a bit in that it puts out an awful lot of information and we do not have so many people to read it all the time. We struggle with bandwidth sometimes, but generally we find it to have good experts and to be very keen to support us in our work.

Rob Shaw: We have a good relationship with it. It has set up a really good graduate scheme with CyberFirst and we are taking people from there. As colleagues have said, we are on CiSP with public and private sector organisations to share information, which is good. It used to be really difficult to work out who you went to in government, because everybody wanted you to go to them until there was a problem; then it was somebody else's problem.

In 2013, when I came into post, nobody looked after healthcare because it was too big, too complicated and, to be honest, too hard. The Cabinet Office, the Treasury, GCHQ, the CPNI, all those different organisations, wanted to know about critical national infrastructure, but in the day-to-day running of the NHS there was no oversight or support from a central organisation. The NCSC has brought that.

My only note of caution is that, when it first opened, I needed to manage my expectations. When we had WannaCry, I expected an army of NCSC staff to appear on the hillside and come in to help us out, but it said, "Where do you want either of our staff?" It does not have a lot of people with the expertise to do things on the ground. Once you accept and understand that, it is fine, but initially I thought it would be a go-to organisation, whereas what it does is signpost you towards the right organisation. It is still in its infancy, but there is some good leadership, which needs to go through the tiers. It has some really good technical people, who are linking well with GCHQ and Ian Levy's team and the techie areas.

There will be times when the NCSC has to take a security view on something and we have to take a healthcare view on it, so I have to have a difficult discussion. That might mean that we have a difference of opinion about how quickly we will put some information out. There needs to be a mature discussion at the right level to be able to make that call. If there was a security issue, I could not, for example, do anything that meant a risk to patient safety. I would always have to make sure that I put patient safety before intelligence going through to a centre.

That is accepted and understood. You would hope that it never came to that, but if we had to do something from a health perspective to protect the patients, that would have to be our priority. How you would make that decision is becoming clearer, but a lot of it relies on specific individuals and their knowledge, rather than what you would do in that type of scenario. That is the only area that I still want finalised.

Q17 **Lord Harris of Haringey:** I have one very specific question for Mr Shaw.

You mentioned that you were not that advanced so you were not that reliant on GPS systems. What about ambulance services? Can they cope without GPS now?

Rob Shaw: Ambulances have their own CAD system. They use GPS to know where they are going, but they have a CAD system that links to their base, as the police have. Some ambulance services' CADs have fallen over, but they have well-tested business continuity planning in place. But you are right that there is an impact. If you are at the top of Oxford Street and you have to get to the bottom of it and there are roadworks, if your satnav is not working you have an issue and you are back to radios, but there are business continuity plans in place. We are not reliant in that if a satellite went down it would not be a disaster, but you are right that we use them for routing.

Q18 **Lord Harris of Haringey:** Martha Lane-Fox asked about your relationships with the NCSC. What about the relationship with regulators? Are you educating the regulator, or is the regulator educating you?

Peter Gibbons: As an arm's-length body of the DfT, our security regulator is the DfT. It released a revised version of railway security regulations in June last year, which included a new section on cybersecurity. Network Rail supported it in drafting that section, so we work closely together. There are some questions about skills and capability. There is a challenge in attracting and retaining good people in cybersecurity, because there are not very many of them and they command very large salaries. Getting some stability of cybersecurity resource in government departments will be a great help. But, absolutely, we are on the same page.

Lord Hamilton of Epsom: Is the regulator a help or a pain?

Peter Gibbons: They are a help. The national railways security programme sets out the requirement for us to secure the railway from acts of violence—largely terrorist attack—but recognises that the sorts of controls you might put in place to prevent a terrorist attack also prevent other types of attacks. Having that regime in place helps me make sure that our business is doing everything that it should be doing to secure the railway.

Lord Harris of Haringey: What about Ofgem?

Phil Sheppard: I will talk about government first. We have very strong relationships with the energy cybersecurity unit that is part of BEIS and the energy resilience and emergency response teams. So BEIS is the regulator that advises us on threats as well as the other aspects, and makes sure that we discharge all the security activities.

Ofgem is a regulator. The current regulatory deal is not very flexible. Over the past four years, we have had, and will have for the next three and a half to four years, discussions about funding for the existing investments. Ofgem published its consultation last week on the next regulatory price control from 2020-21, so we will work with Ofgem to

introduce more flexibility. Part of that process is working with stakeholders, consumers and advocacy bodies to say that these are the levels of resilience that we can spend money on: what is the right level and how quickly do we need to spend some of that investment?

Lord Harris of Haringey: The reality is that if it is not written in, you are much more limited in what you can do.

Phil Sheppard: The National Grid board is very aware of cyber, so we are very careful with our investments. We do not spend just because we can but to make sure that we protect the system, both for security benefits for our customers and from a reputation perspective. Later this year, I think in May, we have a price control update when we can go to Ofgem and say, "We have invested extra in these areas and we would like funding for it".

Rob Shaw: In our area, there is not a single regulator, which makes things a bit more complicated, but NHS England and NHS Improvement hold the contracts for the providers of care and they have been really supportive about what we need from a technical perspective. Because they own the contracts, things need to be written into the contracts to make them real, and that is what they have done.

The overall regulator of performance is the CQC—the Care Quality Commission. We are doing two things with it. When the Dame Fiona Caldicott review was done 18 months ago, the Care Quality Commission looked at the security requirement for health providers, so it was involved in setting that, and we are working with it. We were asked to support unannounced inspections. When the CQC does a planned inspection of any hospital, it will assess its cyber preparedness while it is doing the normal inspections in order to assess risk. That means that people cannot prepare for it.

We are doing a pilot between January and March to work out whether that is beneficial. An unannounced inspection is good in one way, but if you turn up and you cannot get on to the network and no one has the administrator password, et cetera, it is a bit more difficult. ***

The regulators are all supportive of this, because no one wants this to occur in the NHS, so I think we will end up with a vehicle whereby we can do announced and unannounced inspections, but moving more from unannounced to announced inspections so that hospitals know we are coming. An exam question is always easier to answer if you know the question. We do not want people to fail; we want them to hit the level we are asking them to hit.

Q19 **Lord King of Bridgwater:** Can I ask you a question about ministerial involvement? Are you conscious of any active ministerial involvement or interest in the cyber field and the importance of cybersecurity in your own areas? Am I right in thinking that in each case you have a different Minister?

Rob Shaw: Certainly in our area we do. We have a weekly meeting with the Secretary of State, and at least once a month we talk about cybersecurity. Lord O'Shaughnessy, the Health Minister, has been to Leeds to see where we run our national cybersecurity centre from. He is actively engaged. He was one of the people who pushed for a re-profiling of the spend budget to make sure that we set the funding aside for cybersecurity. In every other meeting with Lord O'Shaughnessy, he wants to know what the risk is and whether it has changed. We are lucky that we have two IT and cyber aware people in those roles.

Peter Gibbons: We have had less exposure to questions from our ministerial team at the DfT. They get a brief every month from the Land Transport Security team, so my expectation is that the questions are fed that way, but I have not seen questions directly from the Minister.

Phil Sheppard: For us, there are two aspects. First, the Energy Minister sponsors the Energy Emergencies Executive Committee, which has a standing cyber task group that regularly reports via BEIS to the Minister.

Secondly, every time we have a new Energy Minister, which happens reasonably frequently, we host visits at our control centres and we take people through our cybersecurity aspects: how the CNI networks work and how they are isolated. So we have engagement as far as I am concerned.

Lord King of Bridgwater: So you have an introductory meeting.

Phil Sheppard: Yes. Part of the agenda when a Minister joins the energy department is to visit the national control centre for electricity and sometimes the control centre for gas as well.

Lord King of Bridgwater: That is very interesting.

Q20 **The Chair:** This is a peculiar day in the House—very muddled, all sorts of business going on—and I think you were not formally told that the Committee had decided that, because we were not sure whether we would be quorate, with people coming in and out, we would stay in private session.

Right at the beginning I asked whether you wanted to say anything to us, reflecting the fact that initially you wanted to be in private session. One of you did but the other two were not asked, so I will ask you to do that now. Afterwards we will liaise with you about whether there are things that you do want to put into the public domain. Some of the questions about the number of attacks, et cetera, we would have asked you in the public domain as well, but you might not have given us such full answers. Did you want to say anything else to us in your opening remarks, which we cut across because we interrupted you?

Peter Gibbons: No, not particularly, from Network Rail.

Rob Shaw: This is not something that I would want to say in private, but Peter raised the issue of resourcing and our ability to recruit and retain people, certainly in the public sector, who have the right skills to be able

to do this. The days are gone when a public sector worker comes in and stays for life, unfortunately, so you cannot plan for that. We have set up a recruitment and retention premium on top of the salary to try to attract people. We are setting up our own graduate scheme. We are taking people from the NCSC on placement. We are also looking at other areas; one supplier, FDM—there will be others—takes ex-MoD staff and tries to rehabilitate them. A lot of people who worked in signals are great for this sort of work. We are trying to tap into as many different areas as possible.

My nervousness is that, as both Peter and Phil have said, for every one person who is skilled in this, there are currently three jobs, and that is just in this country, not counting abroad. Basically, people can double their salary just by going somewhere else for a short period. We have a real issue in how we recruit and retain that level of capability to future-proof. We can cope with what we have at the moment, but we do not know what will happen in five years. We can work with universities and other areas, but looking at that collectively across government would be really helpful.

Q21 **Lord Hamilton of Epsom:** Mr Shaw, you told Lord Harris that you had provision with your ambulances. Going back to the attack on the Tube in September, or whenever it was, the police switched off everybody's mobiles so they could not ring up their relations, for the quite good reason that they thought they might trigger another explosion. Did the ambulances have shortwave radios on a separate network? What are the limitations of that?

Rob Shaw: It would be better if I got London Ambulance Service to provide you with a full response. Basically, even when the police block signals, the emergency services are still able to access some of the network. They prioritise so that the emergency services can access it. My assumption is that the London Ambulance Service, in the same way as the police, could still hit the frequency. It knows where to switch to. But I can certainly get London Ambulance Service to provide the information, just to confirm that.

Lord Harris of Haringey: When you do so, it would be useful to get its comments on how well it will work when the new Emergency Services Network is operational, which of course uses the mobile phone system.

Lord King of Bridgwater: A telling intervention.

Q22 **Theresa Villiers MP:** My understanding was that our power networks are somewhat more vulnerable than other parts of our infrastructure. What is your assessment of that? Is that correct? If so, are there other areas where the other organisations represented here are perhaps applying cybersecurity measures that you might want to apply in our power networks, too?

Phil Sheppard: The vulnerabilities are slightly different, certainly with the NHS, given the vast range of applications, servers and all the rest.

We have many services and applications but, from a CNI perspective, we create an air gap around them so that they are secure.

One challenge for the whole industry will be that we rely more and more on distributed networks—everything from smart meters, solar on people's roofs and batteries. A key thing is a phrase that was used earlier, secured by design. All these products in consumers' homes—small generators and small CHP plants—have to start with cyber in mind when they are being designed. If not, it will not necessarily be the National Grid control system that is at risk; it could be all the distributed energy that is at risk. If there is sufficient volume and it is hacked, that can cause local outages and wider issues.

Going back 30 years, we had 80-odd power stations and the network was very confined. Now we have thousands of power stations. We have wind turbines scattered round the network. We have small industrial generators that all participate in the electricity market. Going forward, a lot of thought needs to be done by government policymakers, the designer and the supply chain to make sure that all that is designed to be resilient from the outset and is not something that you try to make resilient afterwards. Today we are in a good place. In the future, this will definitely need to be borne in mind.

Theresa Villiers MP: If, as predicted, people start to install smart fridges and ever more internet-enabled devices in their homes, how do you mitigate the risk of that being used as a backdoor into your system?

Phil Sheppard: There will not necessarily be a direct connection or signal between the two, so that is less of a risk. The greater risk is that someone finds a way of turning on 20 million kettles simultaneously. Those sorts of things need to be thought through very carefully to make sure that the smart meters and all the smart IoT devices are designed to be resilient from the outset and are not open so that people can manipulate them, both on an individual consumer basis and in relation to district heating and that sort of thing.

Q23 **Lord King of Bridgwater:** I asked at the start about global risk. Have you had any central government directions about companies not to deal with?

Peter Gibbons: Not that I am aware of.

Lord King of Bridgwater: Would you expect to be informed? Is there a system? The world is full of takeovers, with different people coming in. The Government have a great ambition to get lots of people to invest in this country. ***

The Chair: ***

Lord King of Bridgwater: ***

Peter Gibbons: From a supplier policy procurement perspective, we have a standard process whereby we check all suppliers to make sure

that they meet our cybersecurity requirements beforehand. If the NCSC makes us aware that there is a supplier that we should not be doing business with, that is all handled through our cybersecurity policy. I would not be involved at that level of detail.

Lord King of Bridgwater: Theresa Villiers mentioned the internet of things and all the things that are now online. What about where all that stuff is coming from?

Peter Gibbons: I could not agree more. We are growing the use of connected devices in the rail network. We are starting to use data in a much more intelligent way to manage the infrastructure and to manage the assets. All those products go through a product acceptance process. We go through the right checks—the right penetration tests and risk assessments—to make sure that we are happy with the provenance of anything that we plug in. If there were a kitemark or an NCSC stamp that went alongside those sorts of devices, that would make our life a lot easier.

Lord King of Bridgwater: That is very interesting. Thank you very much.

Q24 **The Chair:** I seem to recall some publicity a while ago about London Transport having bought a whole stack of new communications stuff from a Chinese-owned company. Could that represent a vulnerability to your organisation? I know you are not London Transport, but presumably there are interconnections.

Peter Gibbons: It is much the same process, whether we are buying from Cisco or Huawei or wherever; they will go through that testing to make sure that they meet our requirements. I am not aware of which supplier it was, so I cannot say whether or not we have any of its technology.

This goes back to the comments I made earlier about the cloud. In some cases we may buy technology from a company of less repute on the basis that we are going to use it in a little room in the corner and it does not connect to anything or do anything important, it just happens to do exactly what we need for that purpose, and therefore the risk is far lower.

Lord King of Bridgwater: How much are you dependent on BT? BT has installed a certain amount of quite controversial Chinese equipment. You say that you are dependent on your suppliers. How organised are you to check down the line in that respect?

Peter Gibbons: Again, this goes back to the comments I made earlier about the contractual relationship I have with my direct suppliers and how I require them to check that their suppliers have the right level of security. I am sure that everyone has a phone in their pocket: that represents the work of 1,000 suppliers. Getting to that level of detail about every single component in a system starts to look quite challenging. It is an issue, I cannot deny it.

Q25 **Baroness Lane-Fox of Soho:** How much do you talk to your international counterparts or feel that you are part of a broader group of similar organisations across the world?

Phil Sheppard: There are some safe places, where the Government have agreed that we can share some information. But, obviously, given some of the numbers and some of the countries that I talked about before, we are very limited in who we are prepared to talk to. The co-operation between us and the US security service is very good. Just the UK and the US—that has worked very well. Outside that environment, there is some sharing of information in Europe, but it gets progressively less once you get past a country such as Australia.

Baroness Lane-Fox of Soho: Does it work? Do you find it helpful to talk to other similar national groups?

Phil Sheppard: We are still limited in what we do. The Governments act as clearing houses, so they have peer-to-peer relationships which are obviously much stronger. We often find things out through that route, such as international best practice, lessons we can learn or case studies, rather than necessarily from any originating company.

Peter Gibbons: From a railways perspective, we have excellent relationships across Europe and sit on a variety of groups specific to cybersecurity. One of the large changes we are going through at the moment is deployment of new signalling systems based on a European standard—the European Rail Traffic Management System—so there are cybersecurity groups across the rail infrastructure managers of all of the member states to consider the cybersecurity of those systems and the suppliers that are developing those systems. Certainly across Europe it is very good. More broadly than that, it is much less so. We have far more engagement across Europe, particularly with France, Holland and Sweden.

Rob Shaw: There are a number of international forums, such as CEN, that look at interoperability and standards, particularly across Europe. We have just had our first Global Digital Health Partnership summit, which was hosted in Australia and was attended by 14 different countries and the World Health Organization.

We are all trying to solve the same problems. One of the threads that came out of that is cybersecurity and the way different countries deal with it. ***

The Chair: Thank you very much indeed. As I indicated, the Committee staff will get in touch with you in the coming week to see what you would be happy for us to use in our deliberations. Thank you.