OFFICIAL REPORT
AITHISG OIFIGEIL

Health and Sport Committee

Tuesday 20 June 2017

Session 5

The Scottish Parliament
Pàrlamaid na h-Alba

Tuesday 20 June 2017

CONTENTS

HEALTH AND SPORT COMMITTEE
17th Meeting 2017, Session 5

CONVENER

*Neil Findlay (Lothian) (Lab)

DEPUTY CONVENER

*Clare Haughey (Rutherglen) (SNP)

COMMITTEE MEMBERS

*Tom Arthur (Renfrewshire South) (SNP)
*Miles Briggs (Lothian) (Con)
*Donald Cameron (Highlands and Islands) (Con)
Alex Cole-Hamilton (Edinburgh Western) (LD)
*Jenny Gilruth (Mid Fife and Glenrothes) (SNP)
*Alison Johnstone (Lothian) (Green)
*Ivan McKee (Glasgow Provan) (SNP)
*Colin Smyth (South Scotland) (Lab)
*Maree Todd (Highlands and Islands) (SNP)

*attended

THE FOLLOWING ALSO PARTICIPATED:

Professor Bill Buchanan (Edinburgh Napier University)
Graham Gault (Scottish Government)
Andy Grayer (NHS Ayrshire and Arran)
Andy Robertson (NHS National Services Scotland)
Shona Robison (Cabinet Secretary for Health and Sport)
Penni Rocks (Scottish Government)

CLERK TO THE COMMITTEE

David Cullum

LOCATION

The James Clerk Maxwell Room (CR4)

Scottish Parliament

Health and Sport Committee

Tuesday 20 June 2017

[The Convener opened the meeting in private at 09:30]

Subordinate Legislation

10:05

Meeting continued in public.

Mental Health Tribunal for Scotland (Practice and Procedure) (No 2) Amendment Rules 2017 (SSI 2017/172)

Mental Health (Patient Representation) (Prescribed Persons) (Scotland) Regulations 2017 (SSI 2017/175)

Mental Health (Certificates for Medical Treatment) (Scotland) Regulations 2017 (SSI 2017/176)

Mental Health (Conflict of Interest) (Scotland) Regulations 2017 (SSI 2017/174)

The Convener (Neil Findlay): Good morning and welcome to the 17th meeting of the Health and Sport Committee in 2017. I ask everyone to switch their mobile phones to silent. People may, of course, use them to access social media, but please do not film or photograph proceedings.

The first item on the agenda concerns subordinate legislation; we have four instruments that are subject to negative procedure to consider.

There has been no motion to annul SSI 2017/172, and the Delegated Powers and Law Reform Committee has made no comments on it. If members have no comments, does the committee agree to make no recommendations?

Members *indicated agreement.*

The Convener: There has been no motion to annul SSI 2017/175, and, again, the Delegated Powers and Law Reform Committee has made no comments on it. If members have no comments, does the committee agree to make no recommendations?

Members *indicated agreement.*

The Convener: There has been no motion to annul SSI 2017/176, and, again, the Delegated Powers and Law Reform Committee has made no comments on it. If members have no comments, does the committee agree to make no recommendations?

Members *indicated agreement.*

The Convener: There has been no motion to annul SSI 2017/174, and, once more, the Delegated Powers and Law Reform Committee has made no comments on it. If members have no comments, does the committee agree to make no recommendations?

Members *indicated agreement.*

Information Technology Security

10:06

The Convener: Agenda item 2 is information technology security, under which we have two panels. On our first panel, we have Professor Bill Buchanan, of Edinburgh Napier University's cyber academy; Andy Robertson, who is the director of information technology in NHS National Services Scotland; and Andy Grayer, who is the acting assistant director of e-health and information services in NHS Ayrshire and Arran.

We will move directly to questions.

Clare Haughey (Rutherglen) (SNP): I welcome the panel to the committee this morning. We value your time.

Can you tell us, in layman's language, what happened and why it happened?

Andy Robertson (NHS National Services Scotland): Essentially, there was a release. I do not think that anyone is quite sure yet where it originated, but a virus found its way into the network.

We share a network with England, and are linked into it. We also have linkages into the internet from our national health service network. The virus found its way onto computers, exposing a particular issue that we have in and around some of the software that runs on some machines. The nature of the virus was such that, once it was on those machines, it tried to connect to other machines with similar exposures. The virus found its way through three layers of security: it found its way through a network port that was open, and then found itself with a piece of software that is designed specifically around file sharing, on a machine that had not been patched to the latest level of the Microsoft operating system, so it was able to spread through our network. As has been publicised, the ransomware nature of the virus was such that it was encrypting files of different types on those machines, so it was effectively shutting down those machines as it travelled through the network.

Does that cover what actually happened?

Clare Haughey: Yes—if you are telling me that that is what happened.

Andy Robertson: That is what happened. On why it happened, it was because of the exposures that we—by "we" I mean a number of organisations worldwide—had in our commuter systems and networks.

Clare Haughey: The virus affected multiple systems internationally.

Andy Robertson: Yes—and it affected multiple organisations internationally, because the virus was released worldwide.

Clare Haughey: Why did it affect the computers in healthcare organisations here in Scotland?

Andy Robertson: The organisations that were impacted, including in the health service here, had a number of things in common. As I have said, we were all using a piece of software that shares information among computers. That is fundamental to how the health service operates daily. The health service is highly linked and networked, and data moves around it, which maintains our services on an on-going basis. Some computers in the health service were running that particular software.

We also make use of a particular network configuration in and around our firewalls. In some places, the virus picked one route—a particular port—through the firewalls. I guess that the perpetrators would understand that as being an exposure across the world. The virus was looking for machines that had not been patched up to the latest-version Microsoft software release for those machines.

Clare Haughey: This is common—

Andy Robertson: Anyone who was impacted had the same set of circumstances across their environments.

Clare Haughey: What was the patch that was not applied? Why had it not been applied?

Andy Robertson: My colleague will explain that.

Andy Grayer (NHS Ayrshire and Arran): The Microsoft patch closed a loophole—it closed a network port—that the virus used to attack the systems.

Clare Haughey: In asking my next question, I do so for people who are technologically challenged. I include myself in that category. Are you saying that systems or software systems inherently have loopholes?

Andy Robertson: I will give you some context. The virus reached 1 per cent of the devices that run in the health service. Therefore, for the most part—99 per cent—the machines that the virus could have reached were protected. For varying reasons, 1 per cent of the machines had not been updated with the particular software patch from Microsoft. However, the other two layers of security that we have in our environment would usually be enough to keep the systems secure. We receive patches all the time from Microsoft and other software vendors in order to keep our estate up-to-date and secure. However, each individual organisation that has responsibility for deploying a

patch needs to make local decisions on how often it runs its patching regime.

Clare Haughey: There is no consistency across NHS Scotland.

Andy Robertson: Across NHS Scotland there are 22 health boards, all with their own accountability for managing their IT estate. We all conform to the same policy and, indeed, to the same guidelines and the same best practice, but local decisions need to be made about when to apply patches. Some of those decisions are tied to the particular circumstances in local boards that might be peculiar to specific parts of a local board's estate, so decisions must be managed locally based on local information. Application of some patches requires downtime and, sometimes, an interruption to normal IT service delivery, so for that reason, too, decisions are made locally on how often patches are applied and what the related regime is.

The Convener: You say that 1 per cent of the machines had not been updated for "varying reasons". What are some of those reasons?

Andy Robertson: It could be that the patching regime was due to run the next week or the next month. It could be that something was in testing locally. There could be complications in and around the software that is run. When we receive patches, they need to be tested before we can deploy them. Sometimes, patches that come in for an operating system will have a knock-on effect on applications that are run on them.

10:15

Medical devices come in many shapes and sizes and require operating system computers to be attached to them, which can sometimes provide reasons why it is difficult to keep patches up to date.

The Convener: What exactly was affected? Was it a specific version of an operating system?

Andy Grayer: The press would have you believe that it was mostly earlier operating systems such as Windows XP that were affected, but evidence suggests that Windows 7 was also affected. The problem was not restricted to Windows XP.

Alison Johnstone (Lothian) (Green): Thank you for joining us this morning.

Mr Robertson suggested, in responding to Clare Haughey's questions, that the incident has exposed a particular issue. I would like to direct my questions to Professor Buchanan. Thank you for your evidence, which I found fairly accessible and an interesting read. You suggest that

"The main lesson we have learnt"

from the incident

"is that there is a complete under investment in the delivery of an IT infrastructure in the NHS."

You go on to say that there is a

"lack of integration across the different stakeholders"

and that, in general, we are lagging behind England on infrastructure. You also say that healthcare has

"the poorest track record for computer security"

and that medical records are incredibly valuable to criminals. You paint quite a picture of concern, and it seems that experts in the field, who will enable us to protect ourselves in the future, are in short supply. Was the incident avoidable?

Professor Bill Buchanan (Edinburgh Napier University): The incident was avoidable. The problem was to do with a file-sharing protocol that is used in the Windows operating system that is not needed at all. In many industries, such as oil and gas and finance, virtualised infrastructure is used. In Edinburgh, you will find what is probably one of the most advanced security operation centre infrastructures in the world. Many of our graduates go and work in the finance industry.

The days of computer systems with technicians walking around using discs to patch have gone. These days, there should be dynamic infrastructure with machines being patched every evening. In this incident, the patch was critical—"critical" is the highest level. To use a term from "This is Spinal Tap", it was an 11 in terms of its threat, so systems should have been patched. The threat was well known—there was a race for the industry to catch up with the patch before people who have the skills to make something malicious turned their evil hands to it. We came out of the incident very well—it could have been much more severe.

We need to look at the whole health and social care infrastructure in Scotland, because we struggle to integrate primary and secondary healthcare at present. In England, that has happened much more easily. In London, there is an open data-sharing partnership: they have managed to get all the health authorities to share information, with agreement on what is and is not allowed to be shared. The system includes dentists, community practices, general practitioners, hospitals and so on. In general, it is a more citizen-focused approach. In Scotland, we really struggle even on integration of healthcare with social care.

We need to admit that our systems are legacy systems. We are now in a data age, or an information age, in which data is critical to pre-emptive understanding of whether people's health is at risk. We need a massive increase in spending

not just on computers, but in order to really look at healthcare services and how we provide them to citizens.

Alison Johnstone: Are you hopeful that the attack will be seen as a wake-up call and that we will take action so that such things are avoided in the future?

Professor Buchanan: Yes. Generally, there has been resistance to the use of IT in healthcare, because it gets in the way. That is typically because services have been designed in a way that does not make it easy for GPs, clinicians and nurses—the most important people—to use the systems.

We need therefore to create an ecosystem around innovation in Scotland, and we need to support small and medium-sized enterprises to engage with the NHS and work with clinicians on the best way of analysing the patient pathway. An outage for a day—or a week, as we have seen with BT and Capita—can not only have an economic cost but could lead to loss of life. A large-scale power outage would have a much greater effect than would a simple ransomware attack.

Alison Johnstone: Is there sufficient knowledge of this area in the NHS?

Professor Buchanan: It is difficult for the health service to recruit staff. The finance and energy industries, for example, pick off the best graduates and professionals. It is extremely difficult to recruit, as we do in education, the best security professionals. We are getting there, but there are difficulties with resources.

Moreover, because there are 22 health boards, it is very difficult to manage an incident. We have to corral the different boards with their different systems, and there is a lot of legacy that needs to be dealt with. It is a 10 to 20-year journey that we must go on. We are moving much more to the cloud—not the public cloud, but virtualised architectures that are much more robust and resilient.

The NHS should have warm sites—by which I mean that if there is a power outage in one area, it is possible to switch over to another area. We should also definitely have a cold site, too. The data infrastructure of the NHS should be set up somewhere else in Scotland—indeed, it does not even have to be in Scotland—and we should be able to flip over to that site if there is a major outage.

Alison Johnstone: In your written submission, you say that we need to

"Build systems based on a white-list of trusted systems, and where all other connections and systems are not trusted."

Obviously, it is all about putting in place a structure that helps to prevent such things from occurring in the future.

Professor Buchanan: Most people in security are now realising that instead of having a blacklist of the things that you are not allowed to connect to, you need to have a white list of the things that you should connect to. The NHS system is so critical that it should be locked down, and the least privilege should be given to every service and role. Only by escalating privilege can you move up. The NHS needs to work on what is allowed and then bar everything else. For example, connections to Tor, the dark web and so on should be automatically barred, there needs to be much more responsiveness to attacks, and there must be an instant response team.

Of course, this is not just happening in Scotland. In the United States, service security in healthcare has been rated as being in critical condition at the moment.

Alison Johnstone: Thank you.

The Convener: We were going to run a jargonometer in this meeting—"jargonometer" was not the term that I used, but you will get the inference—and we have just had reference to virtualised architecture, Tor and other such terminology. Can you help us with the term "virtualised architecture", for example?

Professor Buchanan: If something is virtualised, it is not dependent on a piece of hardware such as, say, a computer or processor—your desktop would run in the cloud; it is a piece of software, but it does not actually run on the hardware of the computer. Instead, the computer is used as a portal, which means that people can have the simplest of computers and can still access the most complex infrastructures within the cloud.

That is the way that most companies and businesses work now. You can go anywhere in the world, sit in Starbucks, make your VPN connection—I hate to have to bring up another bit of tech, but it means "virtual private network"—between you and your infrastructure and then run your desktop virtually on your machine. It means that no ransomware or malware files can run on your computer; the virtualised cloud infrastructure can check those things all the time and can update patches at any given moment. Typically, a desktop will be patched overnight. I have to say that I cannot understand why a patch would take six weeks—especially one that was so critical.

The problem with the NHS is that it has distributed around its network so many disparate computers that are still allowed to connect to it. These days, that should not happen; people should be given a certain amount of time to update

themselves to the latest systems, and if that does not happen, they should be taken off the network completely.

The Convener: I will be dropping "virtualised architecture" into conversations all week.

Professor Buchanan: One last thing—I mentioned Tor and the dark web. The ransomware connected straight to the dark web, so it did not go to any normal website—it did not go to any bank or PayPal or anything like that. It then loaded the Tor browser, which is how the dark web encrypts all its traffic so that you cannot see what it is doing. Even if you are watching what it is doing, you cannot see it. It connected straight into the dark web and into a bitcoin infrastructure.

The NHS needs to understand that any connection to the dark web is malicious. It could be that someone is trying to hide something or is downloading a whole lot of patient records. The NHS needs to understand that it should bar anything that tries to hide its path.

Jenny Gilruth (Mid Fife and Glenrothes) (SNP): I would like to go back to the question that my colleague Clare Haughey asked at the beginning about how all this began. How did the virus transfer? Was it via email in the first instance? Andy Robertson spoke about that.

Andy Robertson: We are fairly sure that it did not come in through email or through someone connecting to a compromised website. There are a number of different places that we look at when our defences are breached, and we are fairly sure that it did not come in through an email or through someone clicking on a link to a website that they might have received through an email. We are fairly sure that it came in through our connection into the N3 network—the NHS national network. In Scotland, we are on the SWAN network—the Scottish wide area network, which is used by our health service—but we have a gateway to the English health service through what is called the N3 gateway. The virus reached us through either that connection or the internet, or perhaps both.

Jenny Gilruth: I understand that once a computer becomes infected files are locked and encrypted so they cannot be accessed, and sometimes payment is demanded via bitcoin. Are you aware of anybody in Scotland making a payment via that system? From what I have read, it seems that payment was demanded and, if people did not pay in a certain number of days, the amount would increase.

Andy Robertson: That is the nature of how an attack shows itself to the user of a device. No one in the health service has ever paid a ransom. It is our policy never to pay. I do not know whether anyone from other organisations in Scotland that were impacted paid. The message tries to encourage people to pay quickly in saying that if they do not pay the price will go up.

In those circumstances, we essentially give up on the machine in its current state and restore it to its last good position, according to our restoration policy—we restore the machine to its position prior to its infected state. I believe that we were able to do that in just about every circumstance for the 1 per cent of machines that were impacted.

It is guaranteed that there will continue to be attacks on the NHS and other organisations. Cybercrime is a huge industry and the stakes are being raised every day—we know that. We are going to have to spend more money on our defences.

I agree with Professor Buchanan, but I do not think that the picture of where the NHS is at is as dark as it was perhaps painted. We are taking all the steps that Professor Buchanan sets out in his submission and has mentioned. We were certainly able to recover the health service; the incident happened at 3 or 4 o'clock on a Friday afternoon, and we were able to recover all our key services by Monday morning. One or two subsequent issues that were based on our having had a major incident over the weekend took us a few days into the new week, but we believe that our defences worked fairly well, given the impact that the incident had on the health service. Where we were breached, we were able to recover as per our recovery plans and disaster recovery regimes.

Jenny Gilruth: Not all health boards were affected in the same way—I think that NHS Lanarkshire and NHS Borders were two of the worst affected in Scotland. NHS Lothian, NHS Orkney and NHS Shetland were not affected at all. Do you know why that was the case? You said that it does not relate to the various operating systems. Does it relate to whether boards were directly connected to the N3 network that you spoke about?

10:30

Andy Robertson: All boards are connected to the N3 network.

Jenny Gilruth: That rules that out.

Andy Robertson: The issue relates to the same set of three circumstances: people needed to be using the particular file-sharing software that Professor Buchanan mentioned, they needed to have a certain set of circumstances and rules around their firewall, and they needed to be in a certain position in their patching regime for the attack to impact on them. Those are the reasons why the attack reached the health service at all; the same reasons apply to why some boards were impacted more than others.

Tom Arthur (Renfrewshire South) (SNP): On a scale of one to 10, with one being the least sophisticated and 10 being the most sophisticated, where would you place the WannaCry virus?

Professor Buchanan: It was probably a one or two. The virus had a kill switch. The developers who make malware systems put in kill switches, and the first thing they do is check something. In this case, it checked two domain names to see whether they were registered on the internet. Someone in England found out that it was making that call and registered the two domains and stopped the virus, which killed the virus. It would have been much worse if that kill switch had not been in there, but that was the core of it, so it did not have a great defence. It was probably not created by someone with large-scale investment in creating really malicious infrastructures.

The energy infrastructure in Ukraine has been attacked by fairly complex malware that attacked the control systems. That was the result of quite large investment. It was fairly easy to detect when WannaCry was connecting to the dark web and then to stop the connection; it was not complex malware. The situation could have been much, much worse.

Tom Arthur: Will you sketch out what an attack at seven, eight, nine or 10 on the scale would look like? Do you think that NHS Scotland's IT system has the resilience to deal with an attack at that level?

Professor Buchanan: I would say that such things can be split into four key risks. The first is distributed denial of service, which is very difficult to protect against. That is where malicious agents across the internet target certain systems and consume all their resources so that they fall over and fail. There can then be a domino effect whereby other systems will fail.

A good example is DNS, or the domain name system, where a failure happened in the United States recently. There was a Facebook outage and 500,000 web cameras across the world were infected by malware. They all had the same user name and password. The cameras directed themselves to the DNS infrastructure that resolves the internet protocol address for Facebook and brought down that infrastructure, which meant that nobody could connect to Facebook. That might seem to be trivial, but imagine if NHS systems could not resolve the names of the IP addresses of the systems that they connect to. That attack brought down Facebook for four hours. Denial of service can do that.

A serious malware infection could go to the core of NHS systems and start to switch off or corrupt databases. We have legacy databases, and it is possible for malware to take over a database and encrypt it. Luckily, the computers that were involved in the attack on the NHS were on the periphery of the network, but a piece of malware that was targeted on the NHS in Scotland could target key data elements and bring down the data infrastructure.

The next threat is large-scale data loss. That is where patient records could be compromised in some way and migrated off the network to be sold on to the dark web.

The last threat, and the scariest one for us, is a large-scale power outage. In that case, like it or not, planes will fall from the sky, traffic lights will fail in London and chaos will be caused. We are highly dependent on our IT infrastructure, so if somebody were to trip the power supply for a key resource in the NHS with the result that there was a large-scale power outage, it could cause the whole of the infrastructure to fail.

We hope that that will not happen, although there are things to deal with it if it does. However, looking at the way in which the key critical network connections are organised in Scotland, we can say that we use London a lot. If I communicate with you, the data packet will probably go all the way down to London then come back up again. Therefore, if we were to lose critical connections to the internet—typically, to London—that would bring down our industry, education, health, finance and so on, and the economic effect would be devastating for Scotland. As I said, I hope that there are lots of things in place to deal with that, but I think that having failover back-up routes for network connections and power is a core part of what we need to think about.

The Convener: Do other panel members have opinions on that?

Andy Robertson: Those are all threats, but we are well aware of them. We know about the attack that Professor Buchanan called DDOS, which represents a cyberthreat of a different nature and involves people maliciously trying to bring down websites and internet-facing services.

We also know about the power outage threat, and I can give the committee some reassurance on that. We have an extremely resilient data centre in Livingston; it is a non-London site, and we manage most of our large-scale national infrastructure out of that centre. We have a contract with Atos, which runs the large data centre for us—it is almost a tier 4 data centre. It has two different power cables, so it is resilient in terms of its power supply; it has an uninterruptible power supply battery back-up and it has generators, should they be needed. There are a number of other measures that we would take in a power outage.

I assure the committee that we are aware of the threats that have been outlined and that we have taken steps to deal with them. We carry out wide-ranging work to cover all the threats to the systems that we run in the health service.

Tom Arthur asked about the nature of the attack and how sophisticated it was. It was sophisticated in its simplicity, given the way in which it breached the networks and compromised that particular exposure. You can see that its reach was worldwide; it was not just the health service that had that exposure.

With regard to the more malicious types of attack that we might come under, we have measures in place to protect ourselves against just about every item. The framework that we use contains a broad range of security and safety measures that cover the range of ways in which we might be attacked.

Tom Arthur: As we move seamlessly and inexorably towards the internet of things, we can see that it might have an impact on how we deliver healthcare. We are aware of some of the opportunities that it presents, but will you talk about the challenges and, particularly, the vulnerabilities that are involved in that?

Andy Grayer: The internet of things is already here in the NHS. These days, most significant medical devices in hospitals are computers in their own right and are connected to the network.

One type of mitigation that NHS Ayrshire and Arran uses to combat a threat that is posed by the internet of things is a separate network for medical devices: anything that is not a desktop computer or a server sits on a separate network and has only the appropriate ports open to allow access to the device. Those items include magnetic resonance imaging scanners, syringe drivers and pumps. They all sit on a separate network that we can monitor and control separately to provide assurance about the network services.

Tom Arthur: Are you confident that we have not been vulnerable to the types of attack that we have been discussing?

Andy Grayer: I would never give a 100 per cent guarantee, but NHS Ayrshire and Arran was largely unaffected during the recent incident.

Tom Arthur: Given the sensitivity of a separate network to internet offenders, I assume that special measures, in addition to existing measures, are in place to deal with an attack, given the impact that it could have on patients' wellbeing and, potentially, lives.

Andy Grayer: Absolutely. That is particularly important if we think about radiology devices. Should they start to compromise our corporate network, we can disconnect them from the network and they will still operate as normal. The images would not then be available across the network, so clinicians would need to go to the devices.

Ivan McKee (Glasgow Provan) (SNP): I would like to go back and explore a wee bit further the cause of the attack and the application of patches. Our machines at home, when we get a patch update, ask whether we want to update to the latest version, we click "Yes", and it does it. I had assumed that that is what happened elsewhere, but if I heard Professor Buchanan right, he said that that does not happen and that, instead, technicians wander about with discs to update machines. Is that an accurate portrayal of where we are?

Professor Buchanan: I cannot say exactly. I heard some people say that there were people walking around patching machines. As I said, these days, there should be an orderly patching system. Companies have patching systems that patch all the machines automatically in the evening. The concept of somebody having to go to a machine to update it is archaic and sounds like a 1970s role.

The NHS should have a general policy of watching the analytics and knowing the top 10 things that need to be patched at the time. There is no excuse for missing the recent one. The core infrastructure might have been well protected and patched, but the problem was probably with computers at the periphery of the network. They should not have been allowed to connect to the infrastructure and propagate the ransomware.

Ivan McKee: I understand that—thank you. Would either of the Andys like to comment on that?

Andy Grayer: Speaking for NHS Ayrshire and Arran, I do not recognise the comments that Professor Buchanan has made. We automate our patch delivery, which happens overnight for our core infrastructure and during the day for our peripheral personal computers, and certainly within one week of patches being released. That is evidenced by the minimal impact that WannaCry had in NHS Ayrshire and Arran.

Ivan McKee: You are speaking for NHS Ayrshire and Arran.

Andy Grayer: Yes. I can speak only for NHS Ayrshire and Arran.

Andy Robertson: I can speak for NHS National Services Scotland. We are responsible for guidelines across the other 21 health boards as well as for our own estate. The vast majority—99 per cent—of the NHS's estate in Scotland was unaffected by the virus. In the vast majority of cases, patching is automated—we do not run

around doing updates with discs. When to apply patches is a judgment call—I make that statement up front—based on service delivery, the level of risk and other layers of security that we use to keep safe during a threat.

It would be difficult, now that we have been breached by that virus, for us to say that we hadx it all covered. Obviously, we did not, but ours was not the only organisation to be exposed in that way. We have automated the process as far as we can under the circumstances, but we have 150,000 devices connected to the NHS network in Scotland and we have 3,500 sites to cover, including general practitioners, pharmacists, optometrists and so on, which essentially operate on their own sites with varying levels of connection to our network.

It would be ideal if we could take people off the network if they were not entirely compliant with the previous night's patch, but that would be impractical for an enterprise such as the NHS in Scotland given our scale, complexity and reach.

10:45

Ivan McKee: Just to be clear, then, it might be only 1 per cent, but people still have to go round manually updating patches on some machines.

Andy Robertson: There are very few of those. I bow to Andy Grayer on this as he knows the technical detail better than I do, but I believe that the issue is not so much about physically visiting sites as about deciding to take services down and live without them while patches are applied and maintenance is carried out on less than a regular nightly basis.

Ivan McKee: Is there some kind of measure for, or do you have any visibility of where we are with, the patch updates? You might want to comment on this, but according to Professor Buchanan, the patch should absolutely have been put in place as soon as possible. Clearly there will be degrees of how critical it is to implement certain patches, but is there any visibility across the NHS of where we are with patch updates, or do we not really have that?

Andy Robertson: We would certainly have that at health board level, but I would not have any such visibility nationally. However, each health board is accountable for its IT security, and people in the kinds of positions that I and Andy Grayer are in will understand our areas of responsibility and exactly where we are with patch versions across our estate.

Ivan McKee: Lastly, has anyone estimated the cost to the health service of this attack, the downtime that it caused and the recovery processes that had to be gone through to bring the system back up?

Andy Robertson: We do not have a number to hand right now, but I think that most of the IT resources that went in were sunk costs. We used our own resources and staff for recovery, and we did not have to spend any real, significant amount of money outside of what we already spend on the people, expertise, tools and other resources that we would use to protect and recover our network.

The recovery side of things is important. According to best practice and the advice that we get across the piece, you can protect yourself, but you have to assume that the level of sophistication of these types of attacks will only increase, and you need to be able to recover. As a result, we have already invested in the ability to recover through back-ups, tools and the staff needed in that respect. This is a bit of race, though, and the requirement is going to increase as we move forward and these types of attacks get more sophisticated.

The Convener: You said that you do not have a figure at the moment, but will it exist at some point in the future, or has it just been absorbed internally?

Andy Robertson: We could certainly pull that figure together, based on the amount of time and money that was spent. I would say that most of the work was done through the good will of IT staff who are already in our employ, but the figure could certainly be calculated.

The Convener: Perhaps the fact that you need to rely on the good will of staff in such circumstances is an issue in itself. Anyway, please provide us with that information, if you have it.

Colin Smyth (South Scotland) (Lab): Mr Robertson, you seem to be saying that although you provide central guidance and central examples of best practice, the problem really lies in the fact that there are 22 health boards doing their own thing. Are you saying that, had all the health boards followed the specific guidance that you had issued, this problem would not have happened?

Andy Robertson: Health service IT governance is based on a coalition of the willing. We are not in a position to issue anything and, indeed, we do not audit what happens in local health boards. We try to collect best practice, and I think that boards try to apply that to their own circumstances as best they can. The fact is that some boards were unimpacted by the virus and the incident, and it is fair to say that if all boards had been at the same level as those that had felt no impact, the impact would have been significantly less. As it was, the impact was limited in its reach.

Colin Smyth: I take on board your point that you do not have enforcement, but are you saying that the boards that were not affected were unaffected because they followed your guidance, or was that down to what they did off their own bat? Are you specifically saying that if all the boards had followed your guidance, no boards would have been affected? I am trying to get to the bottom of the situation.

Andy Robertson: Not all boards are at the same stage as the best practice that reaches across the country; different boards are better at different things. There is a picture, and we already understood what that picture looked like. If all boards across the country had been at the same high-water mark, there would have been zero impact.

Colin Smyth: Professor Buchanan said that, in this case, the patch was a must, so you would have known that. Did you issue guidance to boards saying that they should update their systems with that patch as a matter of urgency?

Andy Robertson: I do not think that we issued anything in particular on that patch. Across our estate, which is very large, we receive patches very frequently. It is a daily occurrence for us to get patches for the various types of software that we run. Is that fair to say, Andrew?

Andy Grayer: Yes.

Andy Robertson: The patch that you are referring to did not stick out as going beyond the normal patching that we receive from Microsoft. As I mentioned earlier, we have multiple layers of protective security in our environment. Even if we do not deploy a patch that we receive one night the next night, we have another two layers of security in place. There are different reasons why we would schedule the deployment of such a patch. Ninety-nine per cent of the estate was patched to that level and was covered during the attack. There was nothing unusual about the patch that you are talking about. We would work with our normal patching regime unless there was a true emergency. There was nothing different about that patch, from the point of view of urgency, from those we would normally receive.

Colin Smyth: In his submission, Professor Buchanan comprehensively dismantles where we are in terms of the technology. I will not go into the technical detail, but he says that there is no need for us to use the file-sharing systems you mentioned earlier—we could use a virtual system instead. Why are we not moving towards using that type of system?

Andy Robertson: We are moving towards using that type of system. I can give an example. The GP systems that run in 1,000 GP surgeries across the country have been locally hosted for a fairly long time. We will shortly be going to market to look for the next generation of GP systems, which will run in the cloud, by which I mean that they will be remotely hosted. As Professor Buchanan laid out, they will run in a secure data centre and be accessed across a network rather than being held on computers in GP surgeries.

We are also looking at how we can move our PC estate to secure data centres. I do not disagree with anything that Professor Buchanan laid out, but it will involve a huge investment to transfer our systems to the next generation of computing, which I think you would agree is what the proposed new arrangement represents. The world is moving there, and we are moving there, too. However, as I said, we have a very large estate and a very large number of stakeholders. We have 150,000 devices, 165,000 users and 3,500 sites, so it is going to take time and money to get there.

Colin Smyth: What level of investment will be needed to get us there?

Andy Robertson: I would say that we do not have an end number. I could not quote you a figure at the moment, but I think that it would take a significant amount of money to do that—we are talking about tens of millions if not hundreds of a millions of pounds. To give you an idea of the scale of our spend on IT, we spend around £260 million a year on services across the health service.

Colin Smyth: One of the committee's roles is to look at budgets. The Government will have to look at budgets, too. Given the seriousness of the issue, are you looking at how much it would cost to get to where you need to be?

Andy Robertson: We are working with the Government and boards on our programme of work over the next few years. We will work through what was the e-health strategy board to put forward our programmes of work across a number of fronts such as acute care, primary care, infrastructure, PCs, GPs, our master patient index and patient-facing systems. We have laid out the programme of work and the amounts of money, which would require increased investment over coming years. It is not clear whether that will be available.

Colin Smyth: You know, therefore, how much would be required to deliver that.

Andy Robertson: The figure is an increase of about £15 million a year to ramp up our programmes to move to that new environment.

The Convener: If the increase is £15 million, what would the total be?

Andy Robertson: The spending is on national and centralised projects.

The Convener: You said £15 million is an "increase".

Andy Robertson: We currently spend about £100 million a year on centrally managed programmes that NSS gets involved in. The projection is an increase of about £15 million that would be required for our work to move faster to new environments.

The Convener: Professor Buchanan, have you or your university colleagues made an estimate of what might be spent on that work?

Professor Buchanan: You need to add a zero and maybe another zero. For our core health and social care infrastructure, £15 million is a patch and sticking plaster—it keeps it going. We need to invest massively.

It is good to see the Digital Health & Care Institute making inroads into innovation. More openness is needed in research and innovation to make sure that Scottish SMEs have the opportunity to work with the NHS. That is happening, but if you want things to go faster, you have to support innovation and the growth of companies—great little cloud companies—and not go with the old model of large, faceless companies running legacy systems and keeping virtual monopolies on their infrastructures. You need a more open system for review, not to pick faults but to see how best to share. The finance industry in Edinburgh is one of the best security infrastructures in the world—a lot of professionals could give support on how to go from legacy systems to the new health and social care environment. It will grow a new economy.

From a citizen point of view, our health and social care does not really integrate. Why did a company based in Skye have to go to London with its eRedbook? Every child born in London now has an eRedbook, but my grandson has a paper-based Redbook—that is great, but a natural extension is an electronic healthcare record. We have talked negatively about ransomware, but we need to understand how to grow a new healthcare infrastructure designed around the citizen rather than around the NHS and its workflow patterns.

Maree Todd (Highlands and Islands) (SNP): I am excited by what you have said. It would be a huge advantage if data that is collected about an individual citizen belonged to that citizen, who would decide who would look at it and share it. That would overcome one of the massive barriers in healthcare—data-sharing. I worked in psychiatry for 20 years, and people would tell the same story time and again, and get tired and traumatised by having to tell the same story because the data is not shared. Tell me more about your vision and what is required to get there.

Professor Buchanan: We have always found that London is a good role model as a city that really looks after its care. London has a similar sized population—larger, even. There is a defined data-sharing policy across London. London has a demographic that is similar to Scotland—from affluent areas, like Chelsea and Westminster, to more deprived areas.

11:00

We need to understand how the data should flow, but we also need to understand the rights of individuals to privacy. That is a really difficult balance, which involves the citizen understanding what information they should hold and own.

The eRedbook is a building block. It seems natural to go from a paper-based system. When we go into hospitals we see that the early warning score system for risk assessment is still done as a pen and paper exercise, which means that you are not gathering information that could be used to predict illnesses and so on.

There is some good work in Scotland, but we have always found that London is the place where innovation thrives. Scotland needs to foster new infrastructures, particularly around the intergration of health and social care, which seems to be the biggest barrier at the moment. How do we care in the home and how do we ensure that people are not admitted to hospital when they do not need to be? We do that by providing information to the first responders—the ambulance staff—so that they have enough analytics to know, without spying on the patient, what prescriptions the patient is on and the risks that they face. Much of the information needed to make a decision is not medical data but can be socioeconomic data.

We could do things a lot smarter, but that also brings security problems. If we were open as a nation we could create the best infrastructure possible.

Maree Todd: Moving on to the security issues, I am aware that we have spent an awful lot of time talking about a malicious attack on our IT systems, when one of the largest security threats is just human error. What do we have in place to protect us against human error? I am thinking of people looking at or being able to look at stuff that they should not, sending emails to the wrong folk and not "blinding" them—all the standard security threats that happen daily.

Professor Buchanan: The top three risks in security are people, people and people.

Maree Todd: As British Airways found out quite recently.

Professor Buchanan: That is right. There is a need for staff awareness. Most ransomware will

come into the system through a phishing email and people clicking on a link that they are not meant to. Most data will be leaked from the infrastructure by, say, a doctor sending an email back to their gmail account and getting the address wrong.

There needs to be a skilling up of all staff in the NHS and across the public sector on how to cope, and there needs to be continual probing. Most companies will carry out some sort of assessment test against their employees, such as conducting a fake phishing attack to see who clicks on it. If someone clicks on it they are sent on a training course. I cannot go into detail on the specifics of that.

Andy Grayer: I can add to that from the perspective of NHS Ayrshire and Arran. We are just about to conduct our first phishing campaign to see how the staff react, where there are flaws and where upskilling and education is needed. We communicate with our staff at various levels on awareness of and education about malware and the associated risks. However, errors do occur—that is just human nature.

On clinicians looking at medical records inappropriately, we use a platform called fair warning, which has been rolled out throughout the NHS in Scotland, which picks up on whether a clinician should be accessing the record of a family member or someone who lives round the corner, for example. That is quite comprehensive and works on an individual basis.

Maree Todd: That happened in emergency care when records were inappropriately accessed by a medic. Was it spotted fairly quickly?

Andy Grayer: It was. Reports from all key systems come back within a month. We move the key systems without staff knowledge and we monitor that. It is quite comprehensive.

The emergency care summary is available to our first responders, but I take Professor Buchanan's point that it could include more social care information.

Maree Todd: It is not available across the board to every health professional who might benefit from using it, such as those in my profession, which is pharmacy.

Andy Grayer: Yes.

The Convener: Maree Todd mentioned the recent situation at British Airways. It appears that a power surge caused the problem and some poor technician is carrying the can for something that happened across multiple sites—dozens, if not hundreds of countries—that brought the airline to a standstill. I assume that British Airways, being a profitable multinational company, had many of the back-ups that the NHS has, which leads me to this question: if it could happen there, can it happen here?

Professor Buchanan: It can happen in any organisation. As I said earlier, we have a complex infrastructure and many systems are dependent on other systems, which are typically outside Scotland and the United Kingdom. A power failure on the east coast of the United States would have devastating effects on the public sector in Scotland because we still run things inside the public cloud. Services such as DNS would also be affected.

Most of the risks are probably external. The concept of the firewall as the main protection for a company is on its way out. In the context of an internet of things structure, the firewall does not really exist. Networks have 3G connections to the internet, so the concept that you can corral a little network and protect it with a firewall has gone.

We need to understand where the data is and what is critical. There is an issue when a device needs to be patched because it has an error—it can take up to a year for a device to be recalled in the NHS.

The infrastructure is very complex. We probably need to be much more dynamic in understanding the internal risks and the external risks. Rather than a loss of profit and face, which is what BA experienced, we would see the loss of life. That is much more important than the brand of a company. We would be measuring a loss in terms of billions if we had a large-scale power outage.

It is great to see that the NHS has things in place, but when something happens you cannot predict exactly what will happen. You might be well-drilled in one area, but something else might happen that you just did not see coming. Increasingly, we need to do more scenario-based training. We need to set up a security range, where we simulate the NHS and find out what would happen if parts of it failed and whether our responders could cope with that.

The Convener: Would anyone else care to comment on that?

Andy Robertson: It is very difficult for us to say that bad things will not happen. However, we can give some assurance about the fact that we realise that. Before I joined the public sector I worked in the private sector for many years and what strikes you when you work for the health service is the straight line between your job and the patient and keeping them safe.

The dependency that the health service now has on IT is enormous. It is very difficult for us to imagine the health service operating without the IT infrastructure. We take that extremely seriously and we put in place fairly broad measures to

protect us, using what the industry is telling us about the best practices around security and resilience.

From the written evidence, you can see some of the connections that we have to the UK and Scotland's best minds on those issues. We try our best to cover the same as everyone else.

The Convener: In 2013, my then colleague, Richard Simpson, asked the Scottish Government:

"what consideration it has given to ending the provision of security support for earlier versions of the Windows operating system and moving to an open source operating system".

The answer that was given was that XP would be unsupported from April 2014 and that

"86% of devices have been upgraded and the exercise will be completed in February 2014."

The answer also said that there was

"no suitably mature, scalable and secure alternative to the Microsoft Windows and Outlook products".—[*Written Answers*, 20 November 2013; S4W-17886.]

Is that still the case? Are there no alternatives?

Andy Robertson: There are alternatives to Microsoft products—that is for sure. However, I will take you back to the scale that I just mentioned. Our installed base is enormous and our investment in Microsoft products is enormous. We will continue to look at alternatives.

What you mean when you say "Microsoft" depends on whether you are talking about the operating systems or some of the software that runs on them. However, Microsoft operating systems are by far and away the predominant operating systems that are used by industries and Governments across the world.

Everyone has the same issue as us: we would like to think that there is an alternative to Microsoft from the point of view of competition and keeping our choices current, but the cost of moving on from a Microsoft-based environment would be enormous and I am not entirely convinced that the benefits would outweigh that.

Professor Buchanan: I think that the concept of an operating system is an old concept. It is legacy. We now have our mobile phones and our iPads. Many of us are running Android and Mac OS. In a decade, the concept of a Windows operating system will seem as old-fashioned as the abacus.

I think that the server infrastructure around the NHS is more likely to be based on a Linux open source platform. Many of the services will be built around that. We need to understand that probably more clinicians and nurses will be using portable devices. They may well use Windows—there are plans for Windows devices—but increasingly, it will be a mobile environment. That mobile environment has 3G connections that do not connect to SWAN and the NHS infrastructure. They are back doors; they are how a clinician can check on the internet to see the best prescriptions and so on.

The day of everything being closed and having a firewall—the idea that as long as the firewall is protecting the whole infrastructure, everything is fine—is the old world. The question that Richard Simpson asked was valid at that time, typically around the cost of licences within the NHS. However, as we migrate, we will be using mobile devices and we will be connecting more and more to the cloud. We really need to understand the changing nature of IT.

Andy Grayer: Ayrshire and Arran territorial board's server estates are probably about 99 per cent Microsoft. That is purely because of our clinical system vendors. They specify Microsoft as an operating system and there are very few alternatives out there, with one notable exception in Scotland. Aside from that exception, they are all Windows.

On Professor Buchanan's point regarding mobile devices, we certainly use a number of mobile devices coming over external networks and we use two-factor authentication to secure the link. That is evidenced in the lack of an outbreak within Ayrshire and Arran. However, we can only run at the pace of the clinical system vendors.

The Convener: On the churn of hardware and software, what is the timescale that you look at in terms of writing stuff off and replacing hardware and software?

Andy Grayer: For desktop PCs in Ayrshire and Arran, we currently work to a five-year timescale. However, due to some financial constraints, that is likely to drift, and for the server estate—

The Convener: Is "drift" another technical term?

Andy Grayer: No—the timescale will drift; it will become a longer period than five years. Our server estate is almost exclusively virtualised and we replace the hosts every five to six years on a rolling basis.

11:15

Andy Robertson: For most of our large-scale national applications that run on the infrastructure, we usually have contract terms of about seven years. However, infrastructure refresh typically runs on a five-year cycle as a default.

The Convener: What would be the accepted IT standard, Professor Buchanan? Is there such a thing?

Professor Buchanan: I would hate to have the problem of moving away from legacy in the NHS. I cannot imagine how that can happen in a relatively short period. However, I know that buying desktop PCs is not the way forward. The minute you put in a desktop PC, you automatically fix something down.

We need to be thinking much more about a mobile-type environment—an IOT environment—and about building systems around the citizen. It will take a lot of investment and a lot of time to do that, so I could not really comment on the cost of replacing PCs.

The Convener: At several points during that, I was just nodding along, pretending that I knew what you were talking about, and I am sure that some of my colleagues were doing so as well. However, I thank the panel very much. It was a helpful session.

11:16

Meeting suspended.

11:20

On resuming—

The Convener: I welcome to the meeting the Cabinet Secretary for Health and Sport, Shona Robison, and, from the Scottish Government, Penni Rocks, the head of e-health (digital health and care) technical strategy and governance, and Graham Gault, also from e-health.

I invite the cabinet secretary to make an opening statement.

The Cabinet Secretary for Health and Sport (Shona Robison): Thank you for inviting me to attend the committee today. I certainly welcome the committee's interest in a significant incident that affected a number of health boards in Scotland. It was a global ransomware attack that was aimed at causing maximum disruption to a large number of organisations across the world. However, it is worth acknowledging the extent of the incident across the UK and, in particular, the NHS.

Across the NHS in England, some 47 health organisations were infected with the malware, including 27 acute trusts. In Scotland, 11 territorial health boards, two national health boards and a number of GP practices experienced some impact from the attack, although that impact was less severe than the impact that was felt in England. We have already learned from the attack that swift co-ordination and the sharing of information limited the impact on the NHS in Scotland. We must all reflect on the incident, identify the lessons that can be learned and, more important, share those lessons with partners so that we can help each other to put in place appropriate and effective measures to combat cybercrime.

I again acknowledge the tremendous efforts of NHS staff and the wider public sector in responding to the ransomware attack and providing assurances around the security of their networks. I reassure everyone that there were no reported breaches of patient data or personal details as a result of the attacks. A UK-wide criminal investigation remains under way, led by the national cybersecurity centre and supported by Police Scotland, and health boards continue to fully support those inquiries.

There are a number of lessons arising from the attack that we must learn. Reviews are under way to capture what can be improved in order to reduce the chances of a similar attack happening in the future. The Scottish Government cyberresilience unit will also arrange a lessons-learned exercise to help health boards and other agencies to mitigate the risks from further ransomware and other cyberattacks.

During this time, there was considerable collaboration across the NHS as well as cross-sector engagement. Collaboration at that level is essential and helps to create confidence in the public sector's ability to respond to such events. Historically, there has been strong collaboration between all e-health leads, e-health infrastructure leads and IT security teams, both nationally and regionally, on IT security issues, with regular meetings being held. NHS National Services Scotland hosts a quarterly meeting called the national information security forum, which is attended by all IT security representatives from each board. They discuss current threats and vulnerabilities and exchange intelligence. That cohesiveness was particularly helpful during the attack, as it allowed security information to be shared quickly and implemented immediately, business continuity ideas to be discussed and good practice to be shared across health boards. Moreover, unaffected boards provided their security expert resource to help those who had been impacted.

Further ideas are being discussed about taking a more national approach to managing IT security across the board and providing systematic and regular intelligence briefings on potential attacks and vulnerabilities. Although we cannot prevent another cyberattack from happening, we will continue to minimise the risk and impact of future attacks.

Initial assessment highlighted that, across health boards, around 1 per cent of devices—around 1,500—were affected. Of that total, some 1,100 were in NHS Lanarkshire, which means that only 400 devices across the rest of NHS Scotland

were affected by the attack. Of the 13 boards that were affected in the NHS in Scotland, NHS Lanarkshire felt the most significant impact, but the board took appropriate precautionary action and, along with other affected health boards, put business continuity arrangements in place to ensure that patient services continued to be delivered across the NHS. Although investigations are still under way in NHS Lanarkshire, early indications are that, although the board's estate and patching regime were appropriate, it had not yet deployed the specific patch prior to the date of the attack. Moreover, it was going through an extensive replacement programme, which is why it was so badly affected. Lessons learned will improve the deployment time of critical patching, and that will be the focus.

There continues to be substantial investment in IT across the NHS. The Scottish Government provides funding of around £100 million per annum to health boards for IT investment and the maintaining of cybersecurity resilience. Health boards spend at least the same amount per annum, although further analysis of health board spending estimates that over £350 million was spent in 2016-17, a similar level of investment is expected this year.

Although the attack was unprecedented in its scope, with hundreds of organisations affected across the globe, it was not an isolated incident. The NHS, along with other organisations, faces similar attacks every day, most of which are thwarted by the controls and protections that are in place. All health boards have IT security frameworks and policies, but the IT environment across health boards is complex, with a mixture of legacy and new systems and technology. Work is continuing to ensure that legacy systems are updated as soon as possible, as developments in technology move on, but some special medical devices still need to run on old IT, and there are challenges around updating them.

Health boards have also put in place appropriate regimes for patching, which is the process of applying fixes from software and hardware suppliers to IT systems in order to improve security. However, I make it clear that the adoption of any patches received from a supplier requires a technical assessment to ensure that there are no unintended consequences for NHS systems. These criminal activities mean that the NHS and other parts of the public sector need to be vigilant and keep their systems up to date and fully protected at all times.

Finally, in response to the attack, the national cyberresilience leaders board quickly convened an extraordinary meeting on 16 May to review the circumstances surrounding the attack and the multi-agency response to it and to identify the next steps to ensure cyberresilience across all sectors. At that meeting, the board agreed to accelerate delivery of a public sector action plan that it had previously been working on to help all Scottish public bodies to develop a shared understanding of and approach to achieving cyberresilience. The board will present the action plan to ministers shortly for their consideration, following which we expect to consult at pace with the wider Scottish public sector on implementation. The plan is expected to include a commitment to develop clear minimum standards of cybersecurity for all Scottish public bodies for implementation during 2017-18 and proposals to provide assurance around higher standards of cyberresilience in key public bodies.

I thank the committee again for the opportunity to be here today, and I look forward to your questions.

The Convener: Thank you very much. In any area of health, there is a tension between services being centralised and different boards having their own systems. However, as the previous panel made clear, this is extremely important life-and-death stuff. Has there been any move towards having a more consistent system across Scotland?

Shona Robison: Yes. I will let Graham Gault say more about that, but it has already been the direction of travel, with our "once for Scotland" approach to IT investment ensuring that our systems are more joined up.

We also want to improve the monitoring of our systems. In my opening remarks, I laid out some of the resilience and oversight that we have at the moment, but there is always room for improvement and it is important that we have that monitoring of systems and continuity.

Graham, do you want say more about the direction of travel?

Graham Gault (Scottish Government): Most of the boards already participate on a co-operative basis. The IT security officers in each board communicate regularly with each other and with others in the other home nations to get the best advice out to all parties at all times. Aside from the impact of standardising security, economies of scale can be achieved by buying product that can be standardised and deployed across all sites and all health boards, and I will be looking at that direction of travel in the coming months.

11:30

The Convener: My follow-on comment is that the words "public sector IT procurement" fill everyone with a chill. Is that just a perception or

the portrayal in the media, or are we really as poor at this as that would suggest?

Shona Robison: You will be aware of the big IT project down south that has become a bit of a legendary tale because it was too complex and it has run into severe difficulties. We have taken a different approach in Scotland, recognising the need to move to more continuity and a once-for-Scotland approach instead of trying to overlay one big system across the NHS, which would bring the challenges that have arisen down south.

Graham, do you want to add to that?

Graham Gault: It is important to note that security products are already purchased under national framework agreements, so all boards will be buying security products consistently from the same vendors. Nevertheless, we must get better at knowing and managing the products on the ground. That is where there needs to be an emphasis on standardisation and more guidance and advice from experts, which we already have through NSS. We have security advisers who lead us through all of this, providing guidance and leadership when attacks happen.

The Convener: In the procurement process, why does it appear that the public purse carries the can for failures in public IT procurement rather than the companies that fail to provide what we want?

Shona Robison: I think that that has improved. In particular, NSS, with its skills around procurement, is able to drive a harder, better bargain on behalf of the public sector. Lessons have been learned from previous contracts in which the balance was not right in that those who were selling had all the information and there was an imbalance of power. We have got much better at that, and NSS's expertise has been really helpful.

Graham Gault: At the end of the day, we are aiming for economies of scale. Larger suppliers may tend to divide and conquer health boards across the nation, so it is important that we keep together. More recently—certainly in Scotland—a lot of the bigger contracts in national frameworks have been a lot more cohesive and well managed.

Tom Arthur: In the previous panel, we took evidence from Professor Buchanan. If I understood him correctly—I caveat my following remarks with that—the trajectory is a move away from fixed desktop infrastructure towards, if I have this right, virtualised architecture and greater use of mobile devices. Does the Government share the view that we are moving towards that?

Shona Robison: There is a move towards what are called cloud-based solutions. Graham Gault will say more about the technical aspects of that, if that is okay.

Graham Gault: Virtualisation is the modern industry way of lowering costs, improving security and increasing the reliability and availability of systems. Most health boards are now virtualising all of their environment for their core components and their core infrastructure, and that is pretty much in place. What varies is how we deliver that, how we manage it on an on-going basis and how we can improve it.

The most important component is the staff training on aspects that are new to people—it is about making sure that staff are up to date. However, the infrastructure across the NHS in Scotland is pretty modern, and that is why the impact of the attack and many of the issues were minimised, certainly from the server point of view. The reporting is about the desktop aspect for the end users, where there were some deviances.

Shona Robison: It may also be worth mentioning the upgrade and replacement of the IT systems that are used by GPs. A procurement is under way, with completion and delivery set for about 2019-20, for new GP and community IT systems. Those will be cloud-based solutions, and they will make a big difference to the way in which GP practice IT systems are configured and how they work.

Tom Arthur: Professor Buchanan stated that he believes that there is a need for significant investment of resources in the overall infrastructure. When the figure of £15 million was cited, he said that we should add a zero and then another zero. Do you recognise that that investment is necessary?

Shona Robison: The figure that I gave in my opening statement was that boards spent £350 million in 2016-17. Over the next five years, their spend will be one and a half billion pounds, which has a lot of zeros.

What is important is how that money is spent. The list of companies and organisations that were impacted by the cyberattack includes multimillion and multibillion pound organisations that spend huge amounts on cybersecurity and IT. For the NHS, what is important is that the resources are spent at the appropriate level and what they are spent on. If we spend billions of pounds on the wrong things, we will not get the systems or the security that we need. What the money is spent on is as important as how much is spent.

Graham Gault: The ambitions of NHS Scotland are significant: we want to do the best job for the population and to deliver efficient and good services. That is a never-ending challenge, so perhaps future investment will reflect the fact that we have an ambitious programme that we want to

invest in to ensure that we deliver for the population.

Colin Smyth: Good morning, panel. Cabinet secretary, you said that you do not think that we were as impacted by the recent cyberattack as the NHS in England was. However, Professor Bill Buchanan from the school of computing at Edinburgh Napier University states in his submission:

"Scotland seems to be behind England in the creation of a robust, modern and dynamic health care infrastructure ... There is a general lack of citizen access ... with weaknesses around the integration of primary and secondary health care, along with a general lack of integration with social care."

Is that a fair criticism?

Shona Robison: I do not think that it is. All our health systems were impacted in one way or another, and we all need to learn lessons from one another. Aspects of cybersecurity in England and Wales might have been better than ours, but the four nations need to learn lessons from one another, and a lot of work is going on at a UK level to make sure that those lessons are learned and that there is co-ordination.

On the citizen-access issue, a lot of work is going on in Scotland. The GP SPIRE—Scottish primary care information resource—programme is a good example of taking the public with us. It is a big, new data system and it is important that the public understand its purpose, so a lot of work has been done to explain that to the public. As I mentioned, the investment in the new GP and community IT systems is very much about linking up primary and secondary care. That cloud-based solution will be at the cutting edge of technology, and procurement is well under way.

If we look across NHS England, there will be pockets of good practice that we would want to learn from, but the system is quite disparate and is not particularly joined up—trusts do their own thing. I am not sure that I would make the comparison in the way that Professor Buchanan has made it.

Graham Gault: There are 22 health boards in Scotland, and we meet every month, as a group of professionals, to share and work together to make sure that we are all bringing services to the fore, that nobody is falling behind and that any new technologies are well discussed and embraced. Sometimes we do trials in one health board area and share the information across others. We are a very cohesive group. I hope that the committee will recognise that that brings a lot of strength and structure to how we deliver our services.

Colin Smyth: However, it is clear from the evidence that we heard earlier, and even from looking at the impact on health boards, that some health boards were impacted more than others. It is clear that whatever best practice guidance we have was not rolled out at the same time by every health board. There are lessons that should be learned. It is not the case that everything happened perfectly at every health board.

Shona Robison: No one is saying that. I think that I said clearly in my opening remarks that we have challenges, that lessons must be learned and that improvements need to be made. There is absolutely no complacency.

Of the 1,500 devices that were impacted, 1,100 were in NHS Lanarkshire. As we now have more information, I tried in my opening statement to give a bit of analysis of the reason for that. In essence, NHS Lanarkshire was upgrading its systems, and while they were being upgraded, the security around them was not as good as it should have been. That is why 1,100 of the 1,500 devices were in one health board. The lesson is that, when systems are being upgraded, the security around them needs to be better. That lesson will now be learned across the whole system, but it provides some explanation as to why NHS Lanarkshire was impacted more than other boards.

Colin Smyth: Everybody agrees that upgrading our systems to move to a virtual system, for example, will cost a significant sum of money. At present, the Government provides £100 million for IT but, as you said, boards probably spend more than £300 million in total on it. That money comes from other parts of the health service budget. I presume that the Government is setting budgets for the next few years, so what specific assessment has it made of how much it will cost over the next five years to get to where you want to be on the use of virtual systems?

Shona Robison: As I said to Tom Arthur, the spend in 2016-17 was more than £350 million, and we can anticipate a similar level of spend in 2017-18. Even if we were to take that level of spend over five years, we would be talking about more than £1.5 billion. However, as part of the analysis of the lessons learned from the cyberattack, and with the coming IT investment—the new digital health strategy will be launched at the end of the year—we will keep under constant review any further capital or resource requirements.

A lot of resources are already going into the system, and I make the point again that where those resources are spent is as important as their level. That is why the priority for the procurement that is on the go at present, with a completion timeframe of 2019-20, is the new GP and community IT systems, because the interface with secondary care is important. The shift towards doing more in the community and more patients being treated in the community requires the IT

infrastructure to support it. That is why that is a key priority.

Colin Smyth: I hear what you say about the amount of money that is being spent, but Andy Robertson, who is the director of IT at NHS National Services Scotland, made the point that it would require an extra 15 per cent on top of the £100 million to get to where he thinks we need to be, and Professor Bill Buchanan said that we need to add a zero and possibly another zero to that. I am trying to get to the bottom of whether the Government has assessed how much is required over the next five years to get to where it wants to be on IT.

Shona Robison: Those assessments are made continually. Further work is being done now, in the light of the cyberattack, to identify the lessons learned and any additional resources that are needed. That work is going on as part of the detailed analysis of how we improve the level of resilience not only in the NHS but across the public sector. The digital health strategy will lay out the key priorities, and the resources will follow them. We will ensure that the resources are sufficient to do what needs to be done and to meet the need.

We could add zero after zero to the amount that we spend on IT infrastructure and cybersecurity measures, but it would not be effective if we were not spending that money in the right way. Global companies such as Telefónica, FedEx and Deutsche Bahn were all impacted by the cyberattack, and they spend huge amounts of money on cybersecurity. It is a matter of ensuring that we have as much intelligence as we can so that we spend the money in the right way, however much resource we have.

We will keep those things under review. There is a big process of learning the lessons, with a detailed analysis of what more we need to do in the NHS and the public sector, and the resource element is a key component of that.

11:45

Graham Gault: We are no different from any other business in that, if we develop and evolve services for improved efficiency, further investment will be required. The business case must stack up, without question, and we have to take informed decisions on what we invest in and how we invest.

As I said earlier, we have great ambitions for engaging in digital services in the NHS in Scotland. Over time, that will induce more demand on infrastructure and put more demand on security requirements, but those components will be built into how we fund and deliver the case in the future.

Colin Smyth: I do not think that anybody is saying that we should spend money on things that do not work. I will explain what I am trying to get to the bottom of. If you have great ambitions to do what we need to do, I am not entirely sure why you do not know how much that will cost over the next few years.

Shona Robison: We have had to review cyberresilience in the light of the cyberattack. There may be additional costs in that, but the work is on-going. You would expect us to do that in a detailed and forensic way, and that is what we are doing.

There is a prioritisation of the IT infrastructure commitments that have already been made, and that is why we are prioritising the GP and community IT systems. That is all costed and the procurement is on-going, with a delivery timeframe of 2019-20. Within the whole IT infrastructure spend, a series of priorities have been set out. There will be further detail on that for the next five years in the digital health strategy, which will be launched at the end of this year. We will keep the committee informed about that.

The Convener: You mentioned that there has been an IT assessment. Can you provide that to the committee? Will you also provide us with details of the global IT budget and the figure for IT security? If you could follow up with that information, that would be helpful.

Shona Robison: Certainly.

Miles Briggs (Lothian) (Con): I want to follow up on the benchmarking of the IT projects. I was made aware of all year 1 and 2 medical students in Lothian being given iPads when they started working for NHS Lothian, but they report that there is no wi-fi across the Lothian estate, so they have not really been much use. I can see the opportunity there, but to what extent are we looking at infrastructure such as wi-fi across the NHS estate? When will that be in place?

Graham Gault: With the decentralisation of funding, the Scottish Government provides health boards with investment and there is local choice. You are correct to say that what health boards spend money on varies. Some health boards are fully compliant—most of them are across their acute services—while some are not. Some are victims of challenge on things such as paid-for television, for which they might have long-established contracts that they have breached by deploying wi-fi into their acute bed areas. There are lots of complexities, so it is not just a matter of saying, “When can we get wi-fi across all our services?”

It is a complicated picture. The ambition of colleagues in e-health is to mobilise the workforce, again for efficiency purposes, in the acute

hospitals and out in the community, and that will certainly be a focus of our investment.

Shona Robison: It is fair to say that, in NHS Greater Glasgow and Clyde in particular, clinicians' use of mobile devices is advanced. They use them regularly to check up on test results and for communication. On benchmarking, I guess that we need to use that as the standard and get all boards to the standard that we expect. Mobile devices and cloud-based systems are the way of the future and broadband connectivity is obviously a key part of that. It is essential.

Miles Briggs: Another issue, which has been my pet project, is text message reminders for GP appointments. Will you update us on where we are with that throughout Scotland, and on improvements? I think that the latest figures showed that there were 1 million missed appointments.

Shona Robison: Through primary care investment, £2 million has been provided to invest in online services, such as the booking of appointments, and other system enhancements. The GP IT infrastructure that I have talked about will revolutionise the way that the digital element of GP services is organised, and also the interface with secondary care. That has a completion timeframe of 2019-20, but in the meantime work is going on to improve the appointment booking and other systems. People expect a level of IT literacy in the way that they interact with services. We have a bit of catching up to do in our primary care services, but it is a priority.

Graham Gault: I add that the funding that the cabinet secretary mentioned has been decentralised. All the servers that are running in general practice in Scotland have the ability to handle online appointment booking. A choice is made at practice level. Some practices go for such things and some are a little bit more resistant. However, now that positive funding has been made available, we are hoping that things will accelerate.

Miles Briggs: Will that be a postcode lottery? Will some of the 22 boards decide that they want to do that and others say that it is not a priority?

Shona Robison: No. The fact that we are putting in additional funding is a real carrot for boards to go down that route. The investment in the IT infrastructure in general practice more broadly—the big project that will be completed by 2019-20—will encourage the best use of technology. In the interface between primary and secondary care, that will be critical to saving time and sharing information. Patients should get a better and quicker experience because of that infrastructure.

The Convener: We strayed a bit from IT security there.

Clare Haughey: I remind members of my entry in the register of members' interests and place on the record my thanks to the NHS staff who worked through the cyberattack. The committee has received written and verbal submissions about staff working overtime during the attack. We have heard about staff good will and, knowing the NHS staff, I am sure that many of them worked above and beyond what was expected of them. With that in mind, will the witnesses tell me what assessment the Scottish Government has made of the impact that such an attack has on staff wellbeing? What steps can be taken to ensure that staff wellbeing will not be compromised should a similar situation arise?

Shona Robison: A huge effort went in over the weekend of the cyberattack. I know that because I was involved in many calls early in the morning and late at night. Staff were working right through the night in some cases, particularly in Lanarkshire. I pay particular tribute to the staff. It was all hands on deck, as it often is in the NHS—that tends to be what happens.

Due recognition has been given. We have written to boards asking for my thanks to be passed on to all staff, but particularly those who went beyond the call of duty, and we expect boards to recognise those efforts. We have not had any information about there being any impact on staff wellbeing, so I do not have any particular concerns on that. We should acknowledge that such events are unusual. Thankfully, they do not happen every day of the week—touch wood. However, it is important that we ensure that staff are recognised for their efforts.

Graham Gault: The cabinet secretary is right—the attack was totally unprecedented. We were caught at 12.30 on 12 May and it took most of the e-health resource across the entire service to respond, which meant that those staff were not doing what they would normally be doing on a Friday afternoon. There is no doubt that the sharing and support that were co-ordinated through the Scottish Government and NSS—I mention NSS specifically, because it is a fantastic resource—meant that we were working as a team. It got to the point at which a lot of the teams were even willing to go to other health boards. I know that NHS Lothian staff went down to NHS Borders to help staff there to get through the blip of the challenge. Going forward, planning and more sharing and knowledge transfer are key.

Clare Haughey: My constituency sits within NHS Lanarkshire, so I am well aware of the difficulties thrown up by the attack.

Professor Buchanan on the previous panel described his thoughts about the way forward and suggested an incident response team. Could such a team help to co-ordinate the response across NHS Scotland?

Shona Robison: We have that already through our resilience arrangements. When something happens, the immediate response team is, if you like, a resilience team. The immediate response team mobilises the right people in the right places, depending on what the challenge is. In this case, the e-health leads were a critical part of that. Those arrangements have stood us in good stead when we have previously had to respond to challenges, whatever their nature. Lessons will be learned about whether we need to tighten up any of that, but I think that our way of responding to such challenging circumstances works pretty effectively.

Graham Gault: We will certainly look a lot more at the levels of defence, protection and, ultimately, monitoring of computer networks. The standards, or the banding, are about protecting your assets, which is probably where we are pitching it at the moment.

Importantly, we are getting much more into event management, which is about knowing what attacks are happening and when. That will give us much more control and enable us to identify attacks in real time and do something about them. In the coming months, we will focus on intelligence.

Alison Johnstone: Professor Buchanan made it clear in his evidence that he is concerned about a lack of investment. He said:

"The main lesson we have learnt from the ransomware attack is that there is a complete underinvestment in the delivery of an IT infrastructure in the NHS."

One key resource is staff. We have been speaking about that, and Clare Haughey raised concerns about the impact on the wellbeing of staff if they are not only working overtime but doing so in a pressured and stressful situation, in which something has gone wrong and they are trying to contain it.

Professor Buchanan spoke about the fact that experts in this field are in short supply not just in healthcare but generally. The challenge is that you are up against huge organisations, with larger budgets to attract the people with the necessary specialist skills. What action is the Scottish Government taking to ensure that we are attracting people? People are attracted to work in the NHS for all sorts of reasons, but are we doing enough to attract people who do not have traditional medical skills but have other skills?

12:00

Shona Robison: It is worth re-emphasising how unusual an event the attack was. Our staff do not work like that in normal peacetime, if we can put it that way. It was a huge cyberattack that required an unusual response. You are absolutely right to recognise the pressure that that put on people, but as Graham Gault said earlier, the response was absolutely fantastic and first class.

It is absolutely true that expertise is in short supply. We need to attract to the public sector, not just the NHS, people who are at the cutting edge of understanding cybersecurity. That means competing with private sector organisations to get the right people. There are programmes of work in which people who have particular skills are brought in to test whether systems are as resilient as they should be.

Graham Gault might want to say something about personnel.

Graham Gault: You touched on a real point, Ms Johnstone. We collaborate across all the health boards, so nobody gets stuck or finds themselves not knowing what to do. There are security forums, gatherings and monthly meetings. The support that the guys give one another is really positive.

I do not hear people saying that they cannot get security officers. We grow our own. We have a unique environment. We have a very complicated IT environment and the model of sharing is important. Also, as the cabinet secretary says, significant use is made of external professionals. I do not apologise for that. The industry—the experts and the technologies that we have to deploy—is changing so fast that it is difficult to keep up to speed. We undertake external penetration testing. That is when we go out and hire external ethical hackers to try to penetrate our networks. We learn much from that and take their guidance and direction.

We have a big package of approaches to solving what you identified as a known issue in the industry.

Alison Johnstone: Healthcare Improvement Scotland spoke of creating a centre of excellence. Is that being considered?

Graham Gault: We are already well down that road. We have experts in NSS who work for Andy Robertson, the IT director. He co-ordinates his team in support of all health boards throughout Scotland. We have expertise at our disposal daily but it is important to enhance skills, training and awareness for those key staff.

The Convener: Did the resilience and contingency planning work as you expected it to?

Graham Gault: As a whole, it is a major success story for NHS Scotland. Most importantly, although there was an impact on patient care—there is no question about that—the recovery time for getting services back to normal was very quick.

The Convener: Yes, but I asked whether you had prepared for such an event happening and whether the preparations that you had made followed through.

Shona Robison: Yes. The resilience arrangements kicked in with everything that goes along with that in terms of a national response. There was also a local response. For example, the move to back-up systems in Lanarkshire worked really well when the IT systems were down. Staff got on to those back-up systems really quickly to minimise the impact on patient care. There was also mutual aid across the system, as we would expect.

Do not get me wrong: there are lessons to be learned about what could have been done better but, had we been laying out the response to a theoretical attack, we would not have been far off what happened, how it was coped with, the recovery time and the analysis afterwards. It would be pretty much in line with the expectation. However, we are not complacent. We absolutely want to ensure that we work even better by learning some lessons from the attack.

The Convener: Thank you very much for coming along. We will suspend the meeting briefly to change the officials.

12:05

Meeting suspended.

12:06

On resuming—

Subordinate Legislation

Carers (Scotland) Act 2016 (Agreements of a Specified Kind) Regulations 2017 [Draft]

The Convener: Agenda item 3 is the consideration of one instrument tat is subject to affirmative procedure: the draft Carers (Scotland) Act 2016 (Agreements of a Specified Kind) Regulations 2017. As usual with affirmative instruments, we will have an evidence session with the cabinet secretary, followed by a formal debate on the motion.

I welcome Shona Robison, Cabinet Secretary for Health and Sport, who does not have her officials with her, and I invite her to make an opening statement.

Shona Robison: Thank you for the opportunity to speak about the draft regulations. It has always been our intention that kinship carers should not be excluded from support for carers under the Carers (Scotland) Act 2016. The draft regulations are to clarify that kinship carers who have a formal agreement with the local authority can be seen as a carer under the 2016 act where they meet the other requirements of the definition.

In particular, the draft regulations will ensure that kinship carers are on an equal footing with parents who would only be seen as carers where the care required is over and above that which would normally be expected for a child of that age. Clarifying the definition of “carer” will assist local authorities to develop their local eligibility criteria under the 2016 act from October. The meaning of “carer” in the 2016 act excludes people who are caring under, or by virtue of, a contract. The draft regulations will ensure that an agreement between a local authority and a kinship carer under regulation 12 of the Looked After Children (Scotland) Regulations 2009 is not a contract for the purposes of defining a carer under the act. Without the draft regulations, those formal kinship carers may be considered to have a contract to provide the care, which would exclude them from the definition of “carer”. Given that kinship carers who have no formal arrangement in place with the local authority cannot be legally considered to be caring under a contract, there is no similar potential barrier to their falling within the definition of “carer” under the 2016 act.

I am clear that there is no suggestion that kinship carers who meet the definition of “carer” in the 2016 act will forfeit any other support that they might receive; any new support under the 2016 act

would be in addition to existing support. It has always been our intention that kinship carers are not excluded from the definition of "carer" in the act, for a number of reasons, and feedback from stakeholders has supported that approach. Kinship carers often find themselves undertaking a caring role after a family member has fallen into crisis; they can feel that they have little choice in the matter when the only alternative is that the child is taken into formal care arrangements. No payment is received for the caring that they undertake; the kinship care allowance is not a fee paid for providing care, such as foster carers receive, but an allowance for accommodation and maintenance of the child or young person in their care. Any support provided through the 2016 act will be aimed at supporting the needs of the carer.

I am clear that kinship carers should not be excluded from the support available to carers under the 2016 act. Therefore, we are introducing the draft regulations to ensure that kinship carers who have formal agreements with a local authority can fall within the definition of "carer" in the 2016 act.

The Convener: As no member has a question to put to the minister, we move to agenda item 4, which is the formal debate on the affirmative Scottish statutory instrument on which we have just taken evidence. Members should not put questions to the minister during the formal debate. I invite the minister to move motion S5M-06069.

Motion moved,

That the Health and Sport Committee recommends that the Carers (Scotland) Act 2016 (Agreements of a Specified Kind) Regulations 2017 [draft] be approved.—[*Shona Robison*]

Motion agreed to.

The Convener: Thank you very much, minister. We now move into private session.

12:10

Meeting continued in private until 12:25.

Published in Edinburgh by the Scottish Parliamentary Corporate Body, the Scottish Parliament, Edinburgh, EH99 1SP

All documents are available on
the Scottish Parliament website at:

www.parliament.scot

Information on non-endorsed print suppliers
is available here:

www.parliament.scot/documents

For information on the Scottish Parliament contact
Public Information on:

Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

The Scottish Parliament
Pàrlamaid na h-Alba