HOUSE OF COMMONS

Public Accounts Committee

Oral evidence: Cyber-attack on the NHS, HC 787

Monday 5 February 2018

Ordered by the House of Commons to be published on 5 February 2018.

Watch the meeting

Members present: Sir Geoffrey Clifton-Brown (Chair); Martyn Day; Luke Graham; Nigel Mills; Layla Moran; Bridget Phillipson.

Sir Amyas Morse, Comptroller and Auditor General, Adrian Jenner, Director of Parliamentary Relations, National Audit Office, Robert White, Director, NAO, and Marius Gallaher, Alternate Treasury Officer of Accounts, HM Treasury, were in attendance.

Questions 1-67

Witnesses

I: Simon Stevens, Chief Executive, NHS England, Sir Chris Wormald, Permanent Secretary, Department of Health, Rob Shaw, Deputy Chief Executive, NHS Digital, Jim Mackey, former Chief Executive, NHS Improvement, and Will Smart, Chief Information Officer, NHS England and NHS Improvement.

HOUSE OF COMMONS

Report by the Comptroller and Auditor General

Investigation: WannaCry cyber attack and the NHS (HC 414)

Examination of witnesses

Witnesses: Simon Stevens, Sir Chris Wormald, Rob Shaw, Jim Mackey and Will Smart.

Q1 **Chair:** Good afternoon, everybody, and welcome to this afternoon's session of the Public Accounts Committee. Today we are considering the NAO Report on the WannaCry cyber-attack and the NHS.

Developments in information technology, including cyber, are increasingly important to the way the NHS functions and to the country in general. However, these developments present challenges and risks as well as benefits and opportunities. This was demonstrated by the WannaCry cyber-attack last May, which caused disruption around the world, including to our own NHS. The attack affected a third of trusts and caused around 19,000 hospital appointments to be cancelled. It also affected 603 primary care organisations and 595 GP practices. The Department of Health—now newly named the Department of Health and Social Care—and the NHS were aware of the threat from a cyber-attack, but were unable to prevent the widespread disruption caused by WannaCry. The NHS was able to manage the attack using existing emergency response arrangements, but we were fortunate that the attack was not more damaging.

This afternoon, we want to get some answers from the Department, NHS England, NHS Improvement and NHS Digital about what they have learned from the WannaCry attack and what action they will take to make sure that they are better prepared to prevent and to recover from any future cyber-attack.

We note that late last week the Department, NHS England and NHS Improvement published their lessons learned review of the WannaCry attack. It may have been a complete coincidence that its publication was just ahead of today's hearing, or it may not; in any case, it builds on the PAC's style of reporting with its 22 recommendations. We need to understand more about the document and its contents, and specifically about how priorities are being set, where the resources are coming from and the timing of interventions. It is far from clear how the implementation of the numerous recommendations in the report will work.

To help us with all that, we are very pleased to welcome our illustrious team of witnesses this afternoon. Starting from my left, we have Rob Shaw, deputy chief executive of NHS Digital, and then Sir Chris Wormald, Permanent Secretary at the Department of Health and Social Care. Sir Chris, you are a frequent flyer with this Committee.

Sir Chris Wormald: I am. This is my 31st appearance, I think.

Q2 **Chair:** Next to Sir Chris, we have almost as frequent a witness, but not quite: Simon Stevens, chief executive of NHS England. Next to him is Will Smart, chief information officer of NHS England and NHS Improvement. Finally, on my right, we have Jim Mackey, former chief executive of NHS Improvement. Welcome, gentlemen.

Perhaps I should start with a general question to Sir Chris. It is a very simple question, really. Can you assure us that no one paid ransom, no person was harmed and there is no future risk to NHS information?

Sir Chris Wormald: The first two of those are covered both in the NAO Report and in Will's report: no one paid the ransom and we did not have any direct cases of patient harm resulting from this attack—though, as you said, there was considerable disruption, which will have affected patients. Can we guarantee future security? No, we can't. Just like in every other organisation, cyber-attacks and cyber-crime are a fact of life. You are never completely safe from them—indeed, if you believed you were completely safe from cyber-crime, it would be an extremely bad sign—so I cannot give you that final reassurance.

While I have the floor, may I pick up on the point you made at the beginning? It is, of course, not entirely a coincidence that we published our response in advance of this hearing. This was work that was already in train—it was a review that we had commissioned after WannaCry—and of course we wanted to be able to be frank with the Committee about what we were actually doing in this space when we came. We wanted to set that out, rather than sitting here knowing there was more to come. So it is nothing to do with this hearing that the report exists, but of course we wanted this Committee to be informed by the results of it.

Q3 **Chair:** Perhaps we might turn to one of our more technical witnesses. Will Smart, how can you be sure that there is no threat to NHS future information from this WannaCry attack? How can you be sure that the virus has been eliminated from all NHS systems?

Will Smart: I do not think we can guarantee that the threat has gone away. In fact, to refer you back to what Chris said, the threat continues. Over the course of the week of the major incident, local organisations put in a huge amount of work. Local staff up and down the country patched systems and put in place changes to firewalls and so on to improve the resilience of the organisation.

In fact, a few weeks after WannaCry, there was another attack that used the same set of vulnerabilities, called NotPetya. That attack impacted a large number of multinational organisations, some of whom had the whole of their IT infrastructure wiped out and had to build it from the ground up again. That used the same vulnerabilities, and the fact that in that case the NHS was not impacted gives some comfort, but it is important that local organisations, national bodies, NHS Digital and others are continually vigilant for the threat as it emerges, and that we take appropriate action when necessary.

Rob Shaw: Could I add to that?

Chair: Of course.

Rob Shaw: As well as NotPetya, we have also had another exact replication of WannaCry with a virus called Bad Rabbit. We have had two attacks that have exploited exactly the same vulnerabilities as WannaCry. No health organisations were impacted by that, as a result of the remediation done as part of the mitigation of the WannaCry attack.

Q4 **Chair:** Thank you. Sir Chris, the Department and the Cabinet Office wrote to trusts in 2014 saying it was essential that they had "robust plans" in place to migrate from old software such as Windows XP. You had thought about this a long time ago, but it seems that somehow that information had not filtered through into action by individual trusts by the time of the WannaCry attack on 12 June 2017.

Sir Chris Wormald: It was a mixed picture. As you say, some action was taken in 2014, and then there was a very big turning point in 2015: the National Data Guardian report and the CQC report, which are referenced by the National Audit Office. A big programme of work was put in place around cyber-crime nationally for pretty much the first time in the NHS. Between that date and the WannaCry attack, a lot of progress had been made. If you look at XP, which you raised, in 2015 I think about 18% of NHS systems used it. That was down to 4.7% at the time of the WannaCry attack, and I think it is now down to 1.8%

However, although a lot of work had been done, at the time of the attack it was work in progress; we had started a programme but we had not finished it. So we were in a better position to deal with the attack at the point that it happened, but by no means a perfect one. We will come on to some of the lessons learned, which Will picked up in his report, among others.

We do have a lot to learn from the attack about how we deal with these things in future, but we were better prepared than we had been two years previously. That is the basic story here.

Q5 **Chair:** Can I examine that? Paragraph 4 in the summary of the NAO Report says, "Prior to the attack, NHS Digital had conducted an on-site cyber-security assessment for 88 out of 236 trusts, and none had passed." So there must have been a red traffic light or a warning alert lingering in your Department.

Sir Chris Wormald: I will ask Rob to comment on this, but the point of those assessments is to identify weaknesses so that they can be improved. It is quite a high bar and, as you say, no trusts had met it. Every trust in the country has things that it can improve around this—even those who do it well. That is the point of the on-site assessments. Of course, we want to get to a position where we are no longer finding things in trusts that need improving, but we are not there yet.

Q6 **Chair:** With great respect, that is quite a glossy answer. None of the

trusts passed the assessment. If a majority had, your answer would have held water, but none of them had. So surely this must have been fairly high up in your in-tray.

Sir Chris Wormald: Yes. To be clear, this had been identified as a big risk. As I say, a lot of action was in place partly for the reason that you say. We had not finished the programme. There were still continuing vulnerabilities, and our assessment of WannaCry and what happened in the incident demonstrated to us that we needed to go much further, so I agree with your basic point. Clearly, there were challenges in the system, some of them known about, which we had existing programmes to deal with. Some of them we learned about from the WannaCry attack and now need to take further action on. Perhaps Rob can add to that.

Rob Shaw: We have now completed 200 on-site assessments. We did 88 before WannaCry. All trusts have still failed, but there are reasons for that. This is not a case of all the trusts having done nothing around cyber-security. On the amount of effort that it takes for NHS providers in such a complex estate to reach the cyber essentials plus the standard that we assess against, as per the recommendation in Dame Fiona Caldicott's report, that is quite a high bar. Some of them have failed purely on patching, which is what the vulnerability was around WannaCry.

We now work with organisations. I always think it is better to have information and know where your vulnerabilities are, so that you can do something about it, rather than hope that you will be okay when you get an attack. These vulnerability reports go back to the trusts and their trust boards, so that they can work out how to do the mitigation. Some need to do quite a considerable amount of work, but a number of them are already on the journey that will take them towards meeting that requirement.

One of the things that we may want to consider now that we have the additional funding available is whether or not we should go back and re-inspect some of those where there is the highest risk, in order to provide ourselves with the assurance that they are going in the right direction.

Q7 **Chair:** Sorry, I made a mistake. The attack was on 12 May, not 12 June, so we are eight months on from that attack. In that paragraph it goes on to say, "However, NHS Digital cannot mandate a local body to take remedial action even if it has concerns about the vulnerability of that organisation." Sir Chris, does your Department have sufficient powers to be able to shake up these trusts to be able to take the necessary action?

Sir Chris Wormald: Yes, we do. They do not fall to NHS Digital. They are in the enforcement powers of the CQC and NHSI, two of the things we had set in train before the WannaCry attack, but they are now in place. The data security standards set by the National Data Guardian are now in the standard contract for NHS trusts, and therefore part of their contract for doing business. This has all gone into the CQC inspection framework, so CQC will inspect against it. The enforcement mechanism would be the same as we use for any other problems that we have in the trusts. It

would be for CQC to report, and then NHSI as the improvement agency would take regulatory action, if need be. It goes into the general system, which is not to say that there were things that we learned from WannaCry that we didn't need to check.

Q8 **Chair:** We are coming on to that, Sir Chris. There will be a raft of questions on that, I am sure.

Rob Shaw: On the CQC, it is worth adding to that. As part of well led inspections, the CQC is also doing unannounced inspections where there is a concern around cyber-security. For a three-month period up to the end of March, we are doing a small number of CQC inspections where we will support them, because obviously the CQC want some technical support to do this. We will do an unannounced inspection on a trust and, as part of that, at the end of March we will then do a lessons learned, in terms of whether that is the right thing to do for an unannounced inspection—not adding a load of burden on to an existing framework, but making sure we get the value out of those inspections.

Q9 **Chair:** The trouble is that each answer is provoking more questions, but I want to bring my colleagues in. Before I do that, I want to ask you a question about the very serious evidence from Martyn Thomas. I don't know whether any of you have had a chance to see it. He was a former director of the Health and Safety Executive. He recently led a cyber-security science capability review for the MOD, so presumably he is quite well qualified in these matters. He makes the point that given that the WannaCry attack was able to encrypt NHS information, it was presumably able to alter NHS information. That could have had really serious implications, such as changing blood groups and that sort of thing. Is that evidence true? If it is, do we think that we are in a position to refute future attacks that are able to do that?

Will Smart: I am afraid I have not seen the evidence that you are talking about, so I cannot comment specifically on it. It may well be true that data can be changed by encryption. It is important to say that every NHS organisation thoroughly backs up all its data, so true copies of that data are available. Copies will be held offsite securely. In fact, after WannaCry, any impacted systems would have been restored from back-ups, because effectively the data was lost. Although there is technical risk, as has been described, in this instance, the data was restored from copies that have been secured.

Q10 **Chair:** So as a minimum, the CQC random inspection should make sure that these trusts—indeed, all organisations in the NHS—are properly backing up their information?

Will Smart: Absolutely.

Q11 **Martyn Day:** Obviously we were quite lucky that it was a relatively unsophisticated attack, but perhaps I could ask Sir Chris or Mr Stevens a question. We had reports in July 2016 from the National Data Guardian and the Care Quality Commission regarding cyber-security. Even as recently as the March and April before the attack, NHS Digital had issued

the CareCERT warnings to update the patch for the Windows operating systems. How come we were so unprepared for it?

Sir Chris Wormald: I refer you to my earlier answer; I do not think that we were completely prepared, and we had a lot to learn from the WannaCry attack, but nor were we completely unprepared. As I said, between the reports that you mention and the date of the WannaCry attack, a lot had happened to implement those reports. As both the NAO Report and Will's report have picked up, there is a lot more that can be done, but we had implemented the vast majority of what the National Data Guardian and the CQC were recommending. We had not finished implementing it. I am not sure that I can add very much.

Rob Shaw: WannaCry was what we call a "zero-day attack". We knew that there was a vulnerability in the Microsoft operating system, but it had never been exploited. We had put guidance out and patching had taken place in more than two thirds of the trusts. They were all secure, or they had the firewalls that protect the network security to prevent vulnerabilities.

We will never mitigate against all cyber-attack. We have to be honest about that. As Chris mentioned earlier, if anybody says that they have mitigated against cyber-attack, it would worry me that they are looking after their IT. We have to look at protection at the front end: we put guidance out, and the trusts that were able to patch, patched. Yes, we have to ask why others had not, but I cannot overstate the complexity of some NHS estates, the size of them and the complexity of trying to patch different parts of them. You can patch one part that can have an impact on something else. The main driver has to be patient care and making sure that we do not have an impact on any of those systems.

We have to look at protection, but also our ability to remediate. We have to accept the fact that things will get through that will cause cyber-attacks on the NHS and social care. How we then respond to those becomes crucial.

Q12 **Martyn Day:** I understand what you are saying regarding the complexities of patching. Clearly, it is not just the NHS itself, but some of the suppliers' equipment that has Windows products embedded. How can you better get them to update their products quickly? Clearly, their machines can be attacked as well as the computer software.

Chair: In answering that, could you address the whole Windows XP point about a lot of the equipment in the NHS?

Will Smart: I wonder if I might pick up on this, and then Rob may want to come back. I would want to start by saying that this was not an attack on Windows XP. Legacy is clearly a challenge in any organisation. The NHS is not unique in having legacy software and devices across the estate. At the time of WannaCry, 95% of devices in the NHS were running Windows 7, which could have been patched, but for whatever reason had not been in every organisation. Legacy is important, but it is not the only issue.

On the reason that patching does not happen, until 18 months ago, I was CIO in a hospital that has a wide range of administrative and clinical services. Clearly, when updating software in clinical areas, it is important to ensure that there are no unexpected consequences to the software or the systems that are running. There is a real challenge in trying to balance the technical risk of knowing you need to do a technical upgrade against the clinical risk to patients as a result of potentially introducing something that may have an effect on a system or a device that is running. We continually balance that. At the Royal Free, where I came from, we had over 10,000 PCs and devices, so these organisations are large-scale, and it is not a trivial case of saying, "We can update all these overnight." There is complexity in that area.

On the point about medical devices, we absolutely faced challenges during the WannaCry attack where we had diagnostic devices with XP software embedded in them that had not been patched. There are two things to say about that: first, we absolutely need to work more closely with software and device providers to ensure that when patches come up, they are in a position to update their very sensitive medical equipment—MRI scanners and so on, which are very sensitive to change—so they have a rapid way to address those vulnerabilities.

Secondly, from an IT management perspective, there are ways of designing the infrastructure in an organisation to protect yourself. Some organisations' networks were effectively completely unsegmented, which is a technical way of saying that everything is connected to everything else, as opposed to separating some equipment from the network and protecting it. There are ways of designing environments to mitigate some of those risks, but it is a hugely complex area. With WannaCry, we saw some of the challenges of managing those issues in that kind of organisation.

Rob Shaw: In terms of XP, it is a really good point. The medical devices are still in support with some suppliers. The operating system is specially written software that uses XP as an operating system. It could take years for them to be upgraded. We have put some guidance out about how you segregate them. The key thing is to take it off the network and make sure that it is isolated, if it is running on something that has the potential to have an impact on other systems. We have put some guidance out on how local organisations can help to mitigate that. In Will's recommendations, there are a number of things that we could go in and check to ensure that the medical devices are properly segregated.

Your point on suppliers is a really good one, because it was mixed. That weekend, we were inundated with suppliers and some of the big systems integrators saying, "Just let us know what you want in terms of support", "We will put boots on the ground", and "There is no question of money or anything like that". A number of the big suppliers helped out in terms of remediation in some of the organisations.

We worked with the National Cyber Security Centre, because once the zero-day attack had become an actual issue, antivirus providers such as

Sophos, McAfee and others had to quickly update their services and systems to prevent future attacks, which they did; they completed that by the end of that weekend. The big systems integrators that provide big PAS and EPR systems for major trusts—some of the American firms—cannot just patch in isolation in one system. They do a patch across their entire estate, and some of those will take time. It is incumbent on us to proactively ensure that if there is a high threat, we do not wait until they tell us that they have patched, but ensure that they are carrying out that patching. Then at least we know where our vulnerabilities lie.

Q13 **Chair:** So Simon Stevens, is there not a simple procurement point here? I wonder whether you will change your procurement processes, so that prospectively, all new equipment procured by your Department is procured on the basis that the software will be supported throughout the life of that equipment.

Simon Stevens: I will bring Will in in a moment, but what we found on the back of the work that was done straight after the WannaCry 12 May attack was that even newly installed equipment systems often had, for example, XP as the embedded operating system. That just emphasises the point that was being made hitherto, which is that getting the firewall right and having system integrity is as important as the componentware, over which we may not have direct control.

Q14 **Chair:** But surely, if you adopted what I was just saying, no manufacturer would be supplying equipment with XP on it because they would not be able to support it?

Will Smart: I was going to say this was a point of clarification, but it may be a point of additional confusion, and I apologise if it is: not all XP is out of support. Where XP is running embedded software within some of the devices, some of that is under support. Going back to the Windows 7 challenge, the challenge is not always whether software is supported or unsupported, but about upgrading that software safely and securely to protect patients from unintended harm as a result of that upgrade. Many of those devices are under support and continue to be supported by the vendor.

Rob Shaw: I think you make a really good point that we can probably do more between our arm's length bodies to support local organisations that are procuring systems, to make sure we give them standard contract clauses that ensure they keep things within the existing, up-to-date and patched, etc. That is probably something we can help with as part of the implementation of Will's report.

Chair: Thank you, Mr Shaw, that is very helpful.

Sir Chris Wormald: There is a wider point prompted by your question. Cyber-security is a whole culture that you need to build into every decision you take, as opposed to saying, "We've bought a system; right, now how do we procure some cyber-security to go with it?" When we look at the trusts that were less, as opposed to more, affected, they seemed to be the

ones that had the wider governance and wider board interest, and that built cyber-security into everything they did.

As you will have heard, an awful lot about securing things was about getting the basics right—had you done your patching and your backing-up? Were your firewalls up to date? Had you isolated things? They were not hugely complicated things to think of, although they can be complicated things to do. An awful lot of this is not about what the IT lead in an organisation does but about the wider leadership. That is true of all organisations right up to the national level.

Rob Shaw: One of the other things we should probably bring out here is that you should not always rely on the contract. Normally, you go to a contract when you get a problem. When we are putting in systems within NHS Digital or any of the systems we oversee, we do what is called secure by design, which means that prior to anything going live, we have a service acceptance criterion that says, "From a business, technical, IG and cyber perspective, have they met the requirements that the business needs?" If we can get that right at the point of go live, it makes some of the remediation far easier, because we know where the gaps are.

Q15 **Martyn Day:** Mr Stevens, how certain are you that no harm was caused to any of NHS England's patients as a result of the attack?

Simon Stevens: No harm has been identified. We obviously have a process for identifying serious untoward incidents, and trusts report if any have arisen. As the NAO accurately reports, that is the position as far as we are aware. That is probably also true in Scotland; although we are principally concerned with England today, as I understand it, 11 out of 14 Scottish health boards and Scottish ambulance services were also affected.

Q16 **Martyn Day:** How long did it take for NHS England to reschedule all the cancelled or postponed appointments?

Simon Stevens: Obviously NHS England itself does not do the rescheduling—that is done by local hospitals and so on—but it would have been within days of the original referrals. By way of context, one patient treatment deferred is one too many, but the NHS looks after 1 million people a day, and the estimate is that perhaps 19,500 of those 1 million appointments may have been affected in terms of outpatients. That is obviously regrettable, but proportionally small.

Q17 **Martyn Day:** Can you quantify the cost to the NHS of the cyber-attack, the postponement of appointments and all the overtime that had to be worked as a result?

Simon Stevens: As the NAO Report says, we haven't got a national estimate of that, and I am not sure whether one has been compiled in Scotland. In effect, a lot of people voluntarily went the extra mile to sort out the situation. It was not only those of us who were involved and spent Friday, Saturday, Sunday and the following week on it. I really want to pay tribute to frontline IT staff, GPs and staff across the hospital systems

and in the national bodies who went the extra mile. Obviously, it was a deep inconvenience, but people put patients first and did that.

Q18 **Martyn Day:** When you say "voluntarily", are you saying that some people worked unpaid overtime to help with the problem?

Simon Stevens: Well, Will for example spent the weekend down at Barts, helping them to direct many people. He did a lot to pitch in. It was pretty remarkable that, by Sunday night, an enormous programme had been put in place to sort out GP surgeries, which obviously came online on the Monday morning. I was in a GP surgery that Monday morning at half 7 to look directly at how the issue was affecting patient care. There was mass mobilisation across the whole of the NHS that weekend.

Q19 **Martyn Day:** I appreciate that your focus is on healthcare rather than the cost aspect, but do you have an idea of how much overtime was accumulated during that period? That would give an approximate estimate of the cost.

Simon Stevens: We don't. As the NAO Report says—and we agree—there isn't a national tabulation of that.

Jim Mackey: To add to that, there wasn't any material increase in overtime over that period, compared with previous periods. As Simon said, generally people did what they needed to do as extra free hours. There would have been some overtime, but at a national level you couldn't really see any different to the normal accounting period.

Q20 **Martyn Day:** I suppose this is a "How long is a piece of string?" question, but how much worse do you think the attack could have been if it hadn't happened on a Friday, if it hadn't been during the quieter period in the summer and if an IT expert hadn't found the kill switch so quickly?

Will Smart: I wouldn't want to hazard a guess, but we can be certain that it would have been worse. There is one statistic that the NAO picked up. After the kill switch was found, we were able to monitor local organisations calling the kill switch. In general, the kill switch was called at the point that the virus was present on the device. It then looked for the kill switch, and if it was there it didn't execute. Twenty-one organisations called the kill switch in the period afterwards, so, in the worst case, 21 organisations may have been impacted. That said, I know that for a number of those organisations—we checked with them—that call was to check that there was a network connection to the kill switch, so it wasn't saying that there was an infection. It would have been worse. We think that perhaps 21 would have been affected, but I would be loth to put a figure on it.

Q21 **Bridget Phillipson:** Can I return to the issue of cost? You have precise numbers about the number of patients who were affected and about the follow-up appointments that would have been cancelled, although it is harder for you to be more precise about some of the aspects of the impact. Why has no assessment been done of the overall cost? Surely having that figure would be helpful in understanding the impact that this has had on the NHS.

Will Smart: It is important to say—we had a conversation with the NAO during their field work—that this data was collected during the incident. The purpose of the data collection was to understand what the impact was and where it was occurring so we could manage the incident most effectively and make sure resources were directed to the parts of the NHS that required support. We did not set out during the incident to enumerate everything about the impact and the cost, because we were focused on resolving the incident. Again, we had a conversation with colleagues in the NAO after the incident while the report was being developed about whether we should do a separate data collection, and we had a relative robust discussion. The view I gave was that I didn't believe that would help us to understand what happened any better than we knew during the incident and I wasn't convinced that it would change those things that we will do in the future to prevent an attack. So that is why we don't know the answer to all of those questions.

Q22 **Bridget Phillipson:** This is probably a question for Mr Stevens. We rightly point out to patients the impact that missed appointments would have on the NHS—the financial cost that is borne when patients fail, for whatever reason, to attend appointments. Would it not be helpful to have a similar exercise here, so that we can understand the impact of failing to get things right on cyber-security?

Simon Stevens: Well maybe, but I think the underlying point is that everybody can see that, on the back of WannaCry, a whole series of things need to change. So, in a sense, that argument has already been won, I think. The fact that we are now explicitly changing the way in which our individual organisations get support, the national infrastructure and targeted investment at cyber-security means, I think, that case has been understood.

Q23 **Bridget Phillipson:** But you don't think it would be helpful for organisations to understand that there is a cost to this?

Simon Stevens: I think organisations would probably sigh a bit if we sent out a new lot of forms nationally for people to try to complete estimating what the marginal costs of an event last May would be. I don't actually think, practically speaking, that would affect the action that now needs to be, and is being, taken.

Q24 **Bridget Phillipson:** But is the same not true of telling patients how much they cost the NHS when they miss appointments? Is that not a waste of time?

Simon Stevens: That is a national estimate; we don't actually do an individual costing exercise for each appointment, because that in itself would be very costly.

Q25 **Bridget Phillipson:** But you frequently do get reminders telling you, "If you fail to attend this very important appointment, this will cost the NHS £120", to give an example. So there are those kinds of figures floating around. All I am saying is that if that is an important driver in patient behaviour, and I am not entirely sure whether the evidence would

support that argument, is it not helpful for organisations to understand that failing to act—in making sure that their cyber-security responsibilities are being discharged—comes with a financial cost as well?

Simon Stevens: Yes, but I don't think that's the principal argument. I think the principal argument here was around patient safety and the continuity of care that the NHS is able to offer. Obviously WannaCry was the first incident—attack—of its kind on a health and care system. We weren't the only organisation that was affected around the world by any means. Obviously, the German railways, the Russian Interior Ministry, Nissan, Renault, the Japanese Government and various others were also affected, so I think it has sent a clear impetus for change and improvement right across the health service, regardless.

Sir Chris Wormald: To add to that, I don't think we've got any evidence that anyone in the NHS was not taking this seriously. So, if you refer to what the CQC and the National Data Guardian wrote in 2016, which was referred to by Mr Day, one of their quotes was, "There was evident widespread commitment to data security, but staff at all levels faced significant challenges in translating their commitment into reliable practice."

I don't think our challenge, even before WannaCry, was persuading people in the NHS that data security is really important; certainly, post-WannaCry I do not think there is anyone in the NHS who would say that. I don't think we do need to prove to people they need to take this seriously. It is about equipping people with the tools to turn that into positive action, of the type that Rob and Will have been describing.

Q26 **Bridget Phillipson:** I understand the point you are making; it's just that the same could be said of a lot of other things. Just in understanding the impacts, sometimes it is helpful for us to understand. No one sets out to have a cyber-attack to which there is an inadequate response, so that people are not fully prepared. However, there are good intentions and then there is making sure you have done what you need to do to set it right.

Sir Chris Wormald: And we agree with that, and a number of the things we have set in place are about ensuring compliance with things that NHS Digital and others send out, for exactly the reason that you say.

On the straight costing question, the truth of it is that it does not fall out of the data we regularly collect from Trusts and others, other than at the very macro level that Jim described earlier. Therefore, to get an accurate number, we would need to do an entirely separate data collection, which would clearly place burdens all the way through the system. For the reasons Will explained, we do not see doing a specific data collection as a particularly positive thing. That is clearly a debatable position—I think the National Audit Office would probably have taken a different decision—but that was the decision that was taken. Ideally, of course, we would have a number, but we don't.

Rob Shaw: I agree exactly with what Chris and Simon said: looking back would not give us any help at all. If I was an ICT director in a local trust, I would want to have some idea, in case this happens again, of how I could make a compelling argument that we should be investing in cyber-security. One of the ways of doing that is saying how much remediation costs. How do you balance prevention and remediation? Looking back would not help, but even if local organisations were able to say, "This is a rough order of magnitude for an attack", that would help them to build their case for what they should be spending on defences.

Sir Amyas Morse: Just to supplement what Ms Phillipson is saying, it would help accountability, however, so it is quite convenient that it has proven not to be practical among all the other things that are practical.

I also think that along with this list of initiatives, it would be a good idea to have a proper costing. There are a couple of one-off numbers, but you do not say what it is all going to cost or whether that is practical in the context of all the pressures on the NHS. It is not old-fashioned or retrospective to say that when these things happen, part of assessing the seriousness of the events—in terms of accountability to Parliament and the practicalities of the forward plan—is to understand to the best of the NHS's ability what the costs concerned are. Nobody is suggesting some exaggerated retrospective thing—just normal accountability with some idea of what the numbers are. I don't think that that is a bridge too far, personally.

Sir Chris Wormald: Since there are clearly strongly held opinions on this matter, I am quite happy to look again at whether there is some non-burdensome way to come to a global number. I don't think it would be an auditable number of the type you normally expect, but I am happy to look at that again, without promising anything.

Sir Amyas Morse: We will face up to the technical challenges of the auditing side.

Sir Chris Wormald: As I say, if there is some way we can manipulate the existing data to give ourselves a sort of global sum, I can see that. What we do not want to do, for the reasons Simon was explaining, is go back to people who take this very seriously and put a further burden on them.

Q27 **Chair:** At this point, could one of you—Sir Chris or Mr Stevens—clarify for the Committee exactly what resources are being devoted to the cyber issue? We have had the whole issue of viring money from the capital budget into the revenue budget. I am not quite sure whether renewal of IT equipment counts as capital or revenue. Perhaps you could just clarify for us what resources you are now devoting to the cyber problem within the NHS.

Sir Chris Wormald: Our spend is divided between what we allocate to IT nationally and what trusts and others choose to spend themselves. Over the spending review period from 2015 to 2020, we have allocated £4.2 billion to IT programmes. Our cyber-security investment nationally—I keep

emphasising that there is a national bit and a local bit—comes out of that £4.2 billion. The original allocation directly to cyber-security within that was £50 million. It was supplemented by an additional £21 million immediately after WannaCry, mainly to deal with systems and infrastructure issues. Then, as part of the reprioritisation we have done since WannaCry, we have allocated a further £25 million this financial year and then £150 million over the following two financial years.

That is our direct spend on cyber-security. Of course, it is very difficult to get to a number for spending on cyber-security, for some of the reasons you raised earlier, Chair. When you upgrade your systems, you are enhancing your cyber-security, and it is frequently better to upgrade your systems than to spend a specific amount on cyber. A lot of the other spending on IT will contribute to cyber-security, but those are our direct investments.

Q28 **Chair:** Can we assume from that answer, because otherwise you would not have commissioned the report that Mr Smart has just produced, with its 22 recommendations, that there will be sufficient funds to implement all his recommendations?

Sir Chris Wormald: We have said—and I hope that this is clear in what we published—that we have reprioritised the £25 million that we will spend this year, and the £150 million, as the initial amount that we will spend on implementing all this. We will keep that amount under review, both in terms of how we are getting on with implementing what Will has recommended and, of course, the assessments of the evolving threat.

I know that does not sound very clear, but at the heart of our challenge is the fact that this is not a static issue. With our friends at the National Cyber Security Centre, we are constantly monitoring what the next set of threats are, and trying to stay one step ahead of people who are playing game theory with us. They are looking at what we have just done, where we have just blocked a potential problem, and where they can go next that we have not thought of. Those are the initial investments we have made, but we will keep that amount under review.

I should add that, as I hope will become clear, a lot of these things are not about money, but culture, practice and systems—though money is, of course, important. Individual trusts, and indeed other institutions in the NHS, are responsible for their own cyber-security and need to invest their own money in it. We are not saying that what we have announced is the sum total of what needs to be spent to protect the NHS. We spend money nationally on: things that go beyond the individual institutions, such as the NHS Spine; things where there is a clear economy of scale, where we can do something on behalf of the system; and things where we are helping to create the framework in which the rest of the NHS can operate well, such as CareCERT and those things that give advice. That is what we allocate central money to.

Resources for the defence of an individual trust or an individual GP come out of their resources, rather than ours. It is quite a complicated picture,

but we try to keep that distinction between what it is right to spend on nationally, and what it is right to leave to local trust boards to deal with in their own circumstances.

Q29 **Chair:** One thing that really concerns me, which comes back to my first words at the beginning of the session, is that your Department has now been given additional responsibilities for the social care sector. I am very concerned, given its diffuse nature, about a cyber-attack on the social care system—for example, if we had large numbers of care homes unable to operate because of a cyber-attack. Are you looking at that whole aspect?

Sir Chris Wormald: We have always had responsibility for cyber-security in social care; that is not something that transferred in with the new name. I will leave Will to say a little more, but one important point is that social care, by its nature, is less technology-dependent than a trust hospital is. I would say that it is much more difficult to defend because of, as you say, its very diffuse nature, but the nature of the threat is probably less, because it is less dependent on high-end IT and diagnostics to run its day-to-day business. Will has looked at some of these questions.

Will Smart: We know that the NHS is made up of a large number of independent organisations—about 8,000 general practices and hospital trusts. There are 20,000 providers of social care across England that range from small, single organisations through to groups, so we know that we have a real challenge.

Actually, we do not have very much evidence about how WannaCry impacted social care. Recommendation 4 in my report is about commissioning research to understand better both the cyber-security stance of social care and, more importantly, to identify what are the right levels of protections that need to be in place in social care, because we do not know that very well.

That said, Health was particularly impacted by WannaCry because of N3, the national NHS network, which connects every NHS organisation together. That was, to the best of our knowledge—Rob can confirm—the route of WannaCry transmission. Those 20,000 social care organisations in general are not connected to N3, so in some senses that provides some isolation.

Local government organisations again were picked up in the NAO Report. No local authority was infected by WannaCry and therefore the impact on that part of the social care network was more to do with challenges around sharing data between health and social care at the interface. So we do need to do more work; we recognise it, and I hope that over the next 12 months we will come back with more detail.

Q30 **Chair:** While you have got the stage, as it were, on that particular subject, you are moving away from the internet N3 system to the NHS email system. What is the timetable for that?

Rob Shaw: That is not the mail system. We are moving away from N3, which is the current network provided by BT. There will be a transition network available while organisations are able to migrate on to the new health and social care network. As more organisations move away, what that does—as Will says, N3 is a single entity, and the health and social care network is a number of providers providing services. So in some ways that will make it easier for us if we got to a situation where we had a mass attack, because it would not attack everybody; it would only be the people on their network. Those transfers are happening over the next couple of years.

Q31 **Chair:** My question was: what is the timetable for when that transformation will be complete?

Will Smart: We think two to three years.

Rob Shaw: A lot of it is speed—how long organisations take to migrate. It is open to them. The first set of organisations have migrated on to the health and social care network, so we have got a number of suppliers now providing those services. What we need to do is ensure we do not end up with a long tail and keep the transition network going for a longer period because organisations are not moving across. There will be some incentives and making sure that people do not languish and become the last one to move across.

Q32 **Bridget Phillipson:** In terms of the response to the attack, why had the plan not been tested for a response to a cyber-attack?

Will Smart: It was purely timing. We had in place plans to test the approach, but unfortunately WannaCry hit before we had a chance to do that.

Q33 **Bridget Phillipson:** Who was responsible overall for leading the response?

Will Smart: Sorry, at which point?

Bridget Phillipson: In terms of the response to WannaCry—

Simon Stevens: On Friday 12th, we decided during the course of the day, when the nature of the attack became apparent, that we would manage this through the emergency preparedness, resilience and response—EPRR—arrangements that we use for any major attack or incident across the NHS. So at that point NHS England stepped up with our partners around the table here to run that as an incident. Since then, we have done a dry run through the kinds of scenarios that we would expect in future type attacks, and we also now have a clear IT-specific cyber operating plan that would kick in if there was a similar event in future.

Q34 **Bridget Phillipson:** So that was not in place then, but you would all now know—

Simon Stevens: That was one of the learnings that came out of WannaCry and one of the actions that has been taken subsequently, yes.

Sir Chris Wormald: The NHS emergency response system that NHS England runs is fortunately very well tested and performs, as it always does, excellently. There was an issue that the NAO picked up about the period before it is declared a major incident and that machinery kicks in, which was about three hours, and we could have been slicker. We have learnt that some things are different in a cyber-attack than in other types of major incidents, which meant we needed specific guidance, which is what Simon referred to, but the EPRR plan basically worked. The issues were before we had escalated to this stage. You see this in lots of crisis situations. One of the biggest issues is when you call it. When does something that happens to be happening in a couple of hospitals, which has been reported, tip over into a major incident and you put the machinery in place? That is always an issue, and it was here.

Q35 **Chair:** Can I challenge the assertion that it worked? The EPRR plan worked with a bit of luck because the kill switch came in and helped you, but people did not know how to communicate with your Department or with your organisation, Mr Stevens; they had to use WhatsApp or mobile phones or whatever. Perhaps that particular document for obvious reasons is not in the public domain, but can you assure us that if a future incident like this happens, people would know how to communicate with your Department and your organisation and that there is a set protocol for doing so?

Simon Stevens: You are right on both points. That is the situation that arose that weekend, and arrangements have been put in place subsequently to deal with that. I don't know how much more you want us to say.

Q36 **Chair:** I don't want you to give anything away. Presumably that document is confidential.

Simon Stevens: Some aspects of it are public and some are not.

Q37 **Chair:** Do you want to say any more, Mr Smart?

Will Smart: NHS Digital colleagues have put in place a system where we now have mechanisms to communicate directly with CIOs across the servers. The CIO community across the NHS has also done a tremendous amount of work in terms of how they join up their networks. They have created a weekly text alert that connects to every CIO and chief clinical information officer across the servers to provide that communication. We have absolutely learnt the lesson that we need multiple communication channels to be in place. Those are now in place and I hope that we don't need to use them for a very long time to come.

Chair: I hope not. Indeed.

Sir Chris Wormald: Just to be clear about what the issue was, the communication system that was in place for EPRR systems, which works with the EPRR leads in individual trusts, did work. One of the things we learnt from the incident is that you need a wider range of people to communicate with. It is not that the plans that NHS England had in place

did not work, because they did; it is that we have learnt that you need more than that, which is what Will is describing.

Chair: I am grateful for the clarification. Thank you.

Q38 **Bridget Phillipson:** Are you now confident that, regardless of where you are in the country, there would be an understanding of where to come in the event of a cyber-attack? The people on the ground would know who to come to, how quickly to do that, and where their responsibilities lie?

Will Smart: Within the handbook we are clear that if there is a suspicion in any organisation that there might be a cyber-attack under way, their first port of call is the NHS Digital data security operation centre. NHS Digital will then triage-assess the risk within an hour of an initial contact with NHS Digital. NHS Digital and I will have a discussion and I will take a decision with the EPRR leads as to how we call it in terms of incident status. We have a process that will proactively manage that in real time.

Q39 **Bridget Phillipson:** Had GDPR been in place when this attack took place, how ready do you think you would have been to respond in a timely fashion to any issues around data breaches?

Will Smart: I think the NHS already has a history of being transparent about that. We report all data breaches. I don't think GDPR impacts the way that we would report those breaches to the ICO and NHS Digital.

Q40 **Bridget Phillipson:** Do you think that the NHS and its constituent parts are ready for GDPR in the broadest sense? Is there an understanding of what needs to be done and about responsibilities and the changes that will need to take effect?

Rob Shaw: Certainly in our organisation, we have a full programme to become GDPR-compliant. Given the type of organisation we are, you would expect that to be the case. We had our internal audit group come in and look at where we were earlier this year, and we have a follow-up in April to ensure that we have a really strong plan to become GDPR-compliant.

Local organisations will all be doing their own planning. There is absolutely no central oversight in terms of whether they are on track to do that—certainly not from my perspective—but we have replaced the IG toolkit that we used to have, which used to put a lot of guidance out about the Data Protection Act and so on. It was one of the recommendations of Dame Fiona Caldicott's review that we relied too much on self-assessment and driving the wrong behaviours, because the toolkit became too much of a tick-box exercise.

We have made it into a data security protection toolkit to try to give local organisations more information so that their boards can help to run the business. It is lighter touch, but the modules in it give more guidance around Dame Fiona Caldicott's principles on GDPR and on the Data Protection Act, and give staff the up-to-date tools that they need. We need to explain to people about things such as phishing attacks, how to keep safe online and how you ensure that you do not fall for mail scams.

As part of GDPR readiness—not of our organisation, but to help the system—we have ensured that as we update the data security protection toolkit, we make it more supportive for organisations that will help towards GDPR compliance. It is down to each local organisation to ensure that it is compliant, in the same way that it is at the moment with the DPA.

Will Smart: Of course, each organisation has the senior information risk owner on the board, who is accountable for those issues at board level. They will ensure that the board is aware of the risks through the information governance alliance, which is a national coalition across all the ALBs. We are publishing information for those organisations to ensure that they are as informed as they can be as to what the risks and regulations are.

Q41 **Bridget Phillipson:** If GDPR had been in place, would you have had additional responsibilities in terms of notifying patients or additional reporting?

Will Smart: I am not sure. Can I write to you to confirm?

Q42 **Bridget Phillipson:** Okay. Sir Chris, where does cyber-security rank alongside your many and varied priorities?

Sir Chris Wormald: It is one of our top risks and it is managed as such. Actually, it is an area where the Department takes a more active role in the setting of the framework and its management than many others that we deal with in Health, mainly because of its cross-Government nature and because we are also interfacing with the National Cyber Security Centre and others. It comes very high up in our risks.

Q43 **Bridget Phillipson:** Do you think the chain of events leading up to the WannaCry attack demonstrate that it is one of your or the Department's top priorities?

Sir Chris Wormald: In terms of priority, yes. The two reports by the National Data Guardian and the CQC that were referred to earlier exist because my Secretary of State asked for them. One of the last things my predecessor as permanent secretary did was to review the IT governance, including the security governance. We put in a new structure, including the role that Will plays, which is to take a look across and work on behalf of all of us on digital and IT issues. I do not think it is the case that there was a lack of priority.

With hindsight, looking at WannaCry, would it have been even better if those things had started earlier and gone quicker? Well, of course, yes. But certainly since 2015, when our national approach on cyber-security began, I do not think that it was an issue of lack of priority. As I have said all the way through this hearing, that is not to say that we do not have huge numbers of things to learn, as Will's report has set out.

Q44 **Bridget Phillipson:** You are right to say that there is always the benefit of hindsight, but is it not the case that we were quite lucky this time because of the timing of the attack, the kill switch and the fact that it was

a Friday afternoon and not in the middle of winter? Had any of those other factors come at different points, the outcome might not have been as positive.

Sir Chris Wormald: We have discussed a number of those things as we have gone along. Clearly, if this had happened at a time when the NHS was under pressure for other reasons such as winter, it would have multiplied the effect. As Simon explained earlier, when you look nationally, quite a small percentage of NHS procedures were in fact affected—somewhere around 1%. If you put that on top of some point when we were under pressure for other reasons it would have had a bigger effect, and in particular places it was much higher than that, but not nationally.

I discussed the kill switch with my colleagues at the National Cyber Security Centre. There clearly is some luck in somebody finding a mitigation, but there is also some science. What happens in these cases is that, as soon as you get an attack, a large number of people across both the public and private sectors look for a tech mitigation. Hopefully, one of that large number of people finds one, at which point everybody else stops. You clearly could have a scenario where none of those people finds something, so we were lucky in the sense that somebody did, but it is not the case that there was only one person looking. As it happens, that individual found one and did so quite quickly, and as described before that clearly mitigated the effect, but there is some science as well as some luck involved in those processes.

Rob Shaw: On the kill switch, as was said earlier, 150 countries were impacted by this. The way the National Cyber Security Centre works is that, whoever finds the kill switch in any of those organisations, the key thing is that it is broadcast as quickly as possible. The fact is that it was found by somebody in this country, a researcher, and NCSC had already unpicked the code. It could have been an hour later or a day later. We also have to make sure that our agreements with other organisations in those other countries are such that, whoever finds the kill switch, the key thing is communicating that quickly so that you can then enact it and reduce the impact of the attack.

Q45 **Bridget Phillipson:** I understand everything you are saying, but in the event that it had taken longer or not happened, what would you have done? What more could have been done then to try to mitigate the impact of the ongoing attack?

Rob Shaw: In terms of mitigation, the EPRR team worked really well. The command and control through NHS England, once we were in that position, worked really well. Simon Weldon, leading it, was telling us where he wanted boots on the ground and where they wanted support. All that was a positive, and a learning experience. If that had not happened, there would have been more business continuity planning that needed to be taken into account, which the NHS practises on a regular basis in terms of crisis management. There could have been more organisations that were impacted, but we knew by then what the impact was going to be. What it was doing was locking out systems, so we knew that once it had

locked those systems it was not changing data or doing anything about exfiltration of data, it was just blocking it. Business continuity planning kicked in and worked really well within the NHS.

Will Smart: I would just like to add that, of course, the kill switch was not the only thing going on to mitigate the effect within organisations. In every NHS organisation up and down the country, IT engineers were working in the server farms, in the network areas and on the PCs to isolate them and ensure that they were as protected as possible. In the period of time from the point at which the infection started, IT organisations were taking steps to protect themselves. We obviously cannot say what the impact would have been had the kill switch not been found, but we know that action was being taken locally and that that action was having some preventive effect on the spread across organisations.

Rob Shaw: The crucial point is that the antivirus suppliers had updated their product set to be able to stop that attack happening. So that weekend, as soon as they knew what that attack vulnerability was, if they had then taken their product and uplifted it so that the vulnerability could no longer be exploited, the number of organisations impacted would have been reduced as long as they had anti-virus in place.

Q46 **Bridget Phillipson:** Turning to the review, what mechanism will there be for agreeing and implementing its recommendations?

Will Smart: I was commissioned by the Department of Health state security leadership board. I presented the report to them. We will meet, I am sure, over the coming weeks to view the recommendations, and they will, no doubt, either accept, amend or reject some of those recommendations. We have a period of discussion and dialogue to go through.

Sir Chris Wormald: We will be using the existing governance mechanisms we use to manage our IT investments and data security to take those forward. It is brought out in the NAO Report that it is a complicated picture; it involves multiple organisations even at the national level, and then, of course, a lot of the implementation needs to be done locally by individual trusts and others. I do not want to downplay the complications, but we think we have a good structure now for bringing together the key players in the NHS and coming to a single agreement. It is that board that does so.

Q47 **Bridget Phillipson:** Mr Smart, of your 22 priorities, are there any that you would seek to draw attention to, if you had to pick out a number of areas of greatest importance or those that would have the biggest impact?

Will Smart: I would obviously say all 22 are critically important. If I were to summarise, leadership is a really critical issue. We need boards to be engaged in the cyber agenda, and we need to make sure that there is appropriate governance within organisations to enable clinical risk, technology risk and operational risk to be properly managed in an

organisation. One of my mantras over the past months has been that boards really need to own this agenda and drive it within their organisation. That is probably one.

Secondly, my first four recommendations are around standards. I have worked in local organisations, and I have done my best to ignore everything that NHS England Improvement has taught me over that time, but we in the centre absolutely need to step in and be much clearer about what good looks like and what our expectations and standards are, and to be more directive—again, the standards on action plans to implement cyber and Essentials Plus, but I also pick out recommendation 2, being clearer about what technology and technical management standards need to be in place in organisations, which I think is really important.

Then, thirdly—rather than going through every one—what we saw in the WannaCry attack was a healthcare environment which was probably much more connected than I think many of us gave healthcare credit for. We saw, particularly when we looked at the 46 affected organisations that didn't have WannaCry infections but were impacted by decisions taken by others to protect themselves, that we have a very interconnected NHS. The recommendation is around looking at business continuity plans beyond the boundaries of your own organisation to understand who you are connected to and what the impact on others will be of decisions that you might take, as well as the impact on your organisation of decisions that they take. That is critical to ensure that in that short period of time when an incident is emerging, we can be confident that the right decisions are being taken about steps.

Q48 **Bridget Phillipson:** That brings us on to recommendation 15, which talks about NHS Digital having the ability to isolate organisations, parts of the country or particular services in order to contain the spread of a virus during an incident. How would that work in practical terms?

Will Smart: Rob and I had a long conversation about that this morning. I think it goes back to the point I just made about business continuity. It is not something that we can just say from the centre: "We are about to switch off large parts of the network." It is particularly where, together with the local communities and organisations, we think there is an emerging threat in an organisation that we take a decision to isolate. Preventively, there is a lot of work that we need to do to make it an option that is safe and practical. It is not something that we would do lightly.

Jim Mackey: Just to add to that, from going back into a provider that was badly affected at the time, it has been really interesting for me to see how boards have really embraced this. I think people have learned an awful lot. They understand their exposure and their interconnections at a regional and national level. You can see an awful lot of board activity on risk.

None of these things are risk free. There is a danger of thinking that this is the only risk that people have to deal with, but simple things like maintaining a CT scanner are not risk free—you can often do simple routine maintenance and then spend several days trying to get the

machine fully up and running again. Boards are grappling with that, but one of the many benefits of this process is that it has made boards much more aware of their vulnerabilities. This cannot all sit at a national level. It is very much about knowing what your own risks are, how you are connected with regional systems and how you respond accordingly to help each other out.

Q49 **Bridget Phillipson:** Sir Chris, do we know how much these recommendations will cost? Is the money there to deliver them in full if that is what the Department decides?

Sir Chris Wormald: Not precisely, no. As I was saying, we made an initial reprioritisation of £150 million to this, but for some of the reasons I explained earlier, we will keep that under review. Taking forward Will's report is one of the things that the digital delivery board, which overlooks the entire programme of £4.2 billion across the spending review, will consider. We have not tried to cost each recommendation individually, but we have made an initial investment of resources. We will keep it under review and take the advice of the digital delivery board about where we need to go in future.

Q50 **Bridget Phillipson:** We know that there will be costs associated with implementing the review, but I suppose what are more difficult to gauge are the unspecified or undetermined costs of a more serious attack of greater magnitude. Although this may involve significant spending, in the long run it might be the right thing to do, not only for patient safety but to save the NHS a lot of money in the event of a more serious attack.

Sir Chris Wormald: Yes, but all these questions raise difficult issues of the balancing of risk. We were discussing some of this outside: the best way to make yourself secure against cyber-attack is to turn everything off, with obvious consequences for patients and others. Likewise, it is possible to spend considerable sums of money and still be vulnerable to attacks. When you look at attacks across the world, they have included attacks on organisations that spend huge sums of money on security or indeed whose whole business is security. Investing wisely is probably more important than the actual quantum, and so are some of the other issues that Will picked out about leadership and the culture of cyber-security. There are clearly investment questions, which is why we have made our reprioritisation, but it is not a problem that can be solved by throwing money at it. You can spend enormous sums of money and still not be secure.

Rob Shaw: We have to make sure that we future-proof this. What we cannot do is throw public money at it and say, "Right—we are now protected against what is known now," when actually we are protecting against the past. We have to make sure that, as things change, we have a well-balanced risk.

It is all about layered protection. You can do something at the front door, but someone may be climbing through your back window at the same time. We have to make sure that as you peel back the onion, you have

different layers of protection in local organisations. Hopefully, with the money that has been allocated, NHS Digital can do more work centrally to reduce some of the systemic risk. It does not make sense for each local organisation to try to monitor vulnerabilities at its perimeter.

On the other part of Will's recommendation 15, at the moment NHS Digital does not know what is deployed in all the major trauma centres, the ambulance services or the big foundation trusts. If we knew what was deployed, we could give really targeted analysis at the level of individual organisations when we got a threat. Instead of general guidance, we could offer something much more specific. I know that recommendation 15 talks about switching people off the system, but the crucial thing is understanding what is actually deployed, and what that threat therefore enounces.

Q51 **Bridget Phillipson:** And that is a big priority for you?

Rob Shaw: It is certainly a big priority for me, yes.

Q52 **Martyn Day:** I have had a look today at your 22 recommendations. Many laudable items are contained in them, but most of them do not appear to have an obvious timeframe. I was wondering if you could give us an idea of where we would expect to be, say, six months from now. Also, how long will it take to complete all 22 recommendations?

Will Smart: We are already undertaking a great deal of work around cyber-protection, remediation and so on as we speak. All these actions will start immediately. Some of them have a longer lead time. Again, we need to have a detailed conversation within the data security leadership board about what the appropriate plan and timescale for that looks like. I would expect that in the next few weeks or months we would be able to come back with a much clearer plan and timetable.

Q53 **Chair:** We are coming towards the end. Can I have a few quick-fire questions, principally to Sir Chris and Simon Stevens? Can you tell us where we have got to with the CareCERT system? How many NHS organisations are now signed up for the CareCERT portal, and how many organisations have registered technical compliance?

Sir Chris Wormald: That is a question for Rob—CareCERT is yours.

Rob Shaw: We have worked with the levers, both with NHS England and NHS Improvement, and all the foundation trusts are now signed up to CareCERT. There are some benefits to that; it is not just a case of signing up and then we can contact them. We are also providing things such as enhanced threat protection. We have a customer service agreement with Microsoft, so that organisations can download patches. About a third of all trusts have downloaded patches from that service. That does not mean that two thirds have not, because this is to support software that was not previously supported. That fits with the one third and two thirds that we had previously.

CareCERT is moving forward. We have put forward a number of things around additional vulnerability scanning, and other things that we can do

with the revised funding that has been allocated. As Will and Chris have said, we need to make sure that we prioritise things in terms of what will have the biggest impact in the reduction of systemic risk for the best value for money. I am pleased to say that through NHS England and NHS Improvement, there is now 100% sign-up from the trusts. The high-risk areas are now all fully signed up to that.

Q54 **Chair:** Sir Chris and Simon Stevens, are you sure in your own mind that both your organisations really have a handle on every single trust's preparedness for a cyber-attack? Are there some out there that are still very unprepared?

Will Smart: We have much better visibility than we had in May about the situation. We are focusing the £25 million second tranche of funding this year on those organisations that still have some vulnerabilities around some of the high-level CareCERTs that were identified, to start to address and remediate issues there. I think we have a good sense of the next group of organisations that we are going to.

We know that some organisations have a lot to do to address all their cyber-resilience issues—Barts, which is a huge organisation, is a good example. We are working hard with them in terms of working through their vulnerabilities, and providing them with funding and support in terms of the work. I think we broadly know which organisations we are most worried about, and we have a plan for a number of them.

Q55 **Chair:** Do you have a number in your head of the trusts that really have a lot more work to do?

Will Smart: I would not like to give a number out. I would be happy to come back with a number if that would be helpful.

Q56 **Chair:** I appreciate that that might be sensitive information, but within the parameters and what you have set out in your 22 recommendations, it is always the worst that have the most work to do. We want to be absolutely certain that you are really on top of those that have a lot more work to do, such as Barts.

Will Smart: We have a list, and we have regular calls within NHS England with the regional teams, and with NHS Improvement staff. In those calls, we go through the organisations that we think are furthest away from having all the technical controls in place that are required. In one sense—this may sound slightly odd—I am almost less worried about those organisations, because they are the organisations that know themselves that they have a distance to go. The worry and the culture and leadership challenge is for those organisations who were not infected during the WannaCry crisis and maybe think, "That is a reflection of the good work our organisation has done". Those are the organisations that we really need to be targeting to ensure that they are really on top of the risks within their infrastructure.

Q57 **Chair:** Is the CQC inspection the only way you are really going to get in-depth knowledge of where each trust is, or have you other mechanisms

to inquire into that preparedness?

Rob Shaw: There is the CareCERT Assure that we carry out on site. We do a full inspection, penetration testing, looking across the full estate. So when Will responds, in terms of CareCERT Assure, that information gets passed to CQC. Before, it was just between ourselves and the local organisations, but as a result of WannaCry that information is now being shared. So CQC can use that as part of their unannounced inspections if they choose to do so, but also NHS Improvement and NHS England, through Will's area, can see the ones at the lower end compared to the ones towards the top end.

Q58 **Chair:** Clearly, at a high level, Sir Chris, a lot of key Government organisations are looking at cyber-security. Are you satisfied that your contacts with all those Government agencies are sufficient for your Department? This is an ongoing science, and you can never rest from it. As you have said before, there are new methods of penetrating IT systems coming along all the time. Are you really sure that all Government agencies are co-ordinating as well as they should?

Sir Chris Wormald: I am unable to promise that all Government agencies have co-ordinated perfectly. Our key interlocutor is the National Cyber Security Centre, who NHS Digital in particular have very close working with. We had close working with them during the cyber-attack, and we worked very closely with them afterwards as well. That is of course a new piece of the landscape, and to be honest it makes it considerably simpler for us that there is a single centre for Government on these issues that we can work with.

Rob Shaw: Only ourselves and the MOD have their own CERT, along with the National Cyber Security Centre. So other Departments rely on NCSC to feed information out and provide information into them. Because we are monitoring the N3 network, the national spine, the mail system and so on, we share information two-way with the National Cyber Security Centre. So some alerts that come from the NCSC originate from what we have seen on our networks. I think that partnership has grown significantly in the last 12 months or so.

Q59 **Chair:** Sir Chris, on the EPRR, at what time did your Department know that the attack was taking place?

Sir Chris Wormald: I think it is set out in the report. It was about 1 o'clock on the Friday that there were the first reports, and I think the national incident was called at 4 o'clock? Is that right?

Simon Stevens: Yes. We declared it at 4 o'clock.

Q60 **Chair:** So if that is the timescale, that sounds like a reasonable timescale on which to be making a decision on a very important national emergency.

Sir Chris Wormald: Yes. As I say, the NHS is very good at emergencies, and that bit does kick in very quickly. We had conversations with the National Cyber Security Centre straightaway, as soon as the first reports

came in—which was also extremely helpful to that decision making. But the decision making—particularly that by NHS England—was very swift indeed.

Simon Stevens: To add to that, the first trusts were reporting to NHS Digital CareCERT by lunch time—1 o'clock. By 4 o'clock, it had become a larger group of trusts, so we declared the cyber-attack a major incident and established a control centre. At 5 to 5, NHS Digital released to the NHS an NHS-wide cyber-bulletin. At 5 o'clock, we briefed the Secretary of State, and then by 6.45 we had initiated the EPRR plans for the single point of co-ordination across the NHS as a whole.

Q61 **Chair:** Thank you for that very helpful answer. Sir Chris, can I challenge one of your earlier answers in which you said that the EPRR worked well in one particular area, and that is in comms? There seems to have been a bit of tension in what you should have been communicating. In some respects, people wanted more information, to know what was actually happening in their NHS, with cancelled appointments and everything else. In another respect, some of the trusts wanted to keep it quiet, because they did not want their particular weaknesses to be exposed, I presume. Have you undertaken a "lessons learned", as it were, for the whole EPRR process, and in particular have you looked at how you would communicate these types of incident in future?

Sir Chris Wormald: Yes. I will say a couple of things and then I will bring Simon in. We review the EPRR process all the time. Now, every time there is an incident that uses the machinery, there are lessons learned and we update it in the light of experience. Just to clarify, what I mean is that the EPRR system worked as it was designed to work. And in that sense, that is of course what you'll want. That is not to say that it was perfect for this incident. Some of the things Will picked up were about how we have to evolve that system in the future.

So, just to be clear about what my previous answer meant, it was that the system worked as it was supposed to work, which is of course quite a good starting place, but that is not to say that it was completely perfect for this incident, and we have learned quite a lot. Simon.

Simon Stevens: All I was going to add to that was that the evolution of it over the 72 hours, from Friday night through Monday morning, was such that the first 24 hours or so were about establishing what was happening technically. Since the principal arrangements then had to be put in place were linked to major trauma and the emergency care system, there wasn't actually a public behavioural response that was needed on the Saturday. And in parallel with that, in any event, the Government—as part of the Cobra arrangements—perfectly understandably decided to communicate through as a security-related incident, and the initial evidence was that that was what it was.

By the time we got to Sunday, obviously we needed to give public advice about whether or not to go to your GP appointment or hospital out-

patients on the Monday, and at that point then the NHS communications publicly kicked in, as they normally would.

Q62 **Chair:** So are you satisfied that the communications were as seamless as they should have been?

Simon Stevens: We have already talked about the mechanisms with individual trusts, GPs and so forth. So I think you made two important points there earlier, Chair, and we accept those. However, as for the public communication, I think that in terms of what the public were being asked to do, yes, by the time we got to Sunday people were getting the right advice for Monday.

Q63 **Chair:** One of the technical issues, I'm advised, on the particular WannaCry virus was the ability to communicate with each organisation's server. If you turn to paragraph 2.12 in the Report, on page 20, you will see that it says, "The Department and its arm's-length bodies also had limited central information on trusts' IT and digital assets such as anti-virus software and IP addresses." It then goes on to say, "At the start of its investigation, the National Crime Agency had to gather evidence from all sites, including information on the devices affected, IP addresses and network traffic".

If the kill switch had not worked, this sort of core central information surely ought to have been something that was pretty readily available either to NHS England or the Department. I am just wondering whether you have now rectified that.

Rob Shaw: That is the point that we said earlier. At the moment, we don't collect that information nationally and I think that is part of Will's recommendation 15; that's one of the things that we should be able to do. We need to understand what IP addresses local organisations work in and that type of thing.

Before we had WannaCry and CareCERT—going back about six to eight months—there was a really simple question: "So who do you write to in the NHS?" So, other than through the regional teams once the EPRR starts to kick in, in terms of tried and tested mechanisms, we didn't have a list of all of the chief information officers, all of the security leads, all of the staff that we needed to put this out across health and social care.

So we have collected that information and we are continuing to evolve the way that we do communicate, and if we were able to get what is deployed locally, then we could really have been able to say, "Right, we now know where that vulnerability lies. We can now give targeted information to those areas." I think we covered it previously, but it was a really well made point in the report.

Q64 **Chair:** When do you expect to be able to be able to co-ordinate all this information?

Rob Shaw: I would have to come back to you with timescales. It was part of Will's report from last week, which we completely support.

Q65 **Chair:** I was going to come on to the timescales. Perhaps either Sir Chris or Simon Stevens could answer when they expect to be in a position to tell us when all of the 22 recommendations in Mr Smart's report will be implemented, and under what timescale? The purpose of that question is to try to work out when the Committee might revisit this whole subject.

Sir Chris Wormald: You're saying six months?

Will Smart: Six months in terms of having a firm plan. Recommendation 1 talks about the Cyber Essentials Plus standard being in place around the NHS by June 2021. That would be the long stop, in terms of when the plan as a whole would finish. We can certainly give you a gradated plan by action over the next few months.

Q66 **Chair:** What I would like to ask of both of you this afternoon is if you would give the National Audit Office a six-monthly update of where you are with the report?

Sir Chris Wormald: Yes.

Chair: We will then know when we ought to revisit the subject.

Sir Chris Wormald: That would be completely appropriate. The point we made throughout the hearing is that, although we will put in dates on actions—it is very important to monitor those—this is of course a job that is never done. It is not as if we will reach 2021, or any date, and declare victory on cyber-security, nor will the things that Will has just published be the last word on what the Government need to do. We will update what we do continuously. However, six-monthly reports to the National Audit Office would be entirely appropriate.

Q67 **Chair:** Sir Chris, I can't find it exactly in the time available, but one of Mr Smart's key recommendations is on people. IT and cyber-security is very much an evolving science, so you will need good, young, trained people. Are you satisfied that the National Cyber Security Centre is producing the number of people with the rights skills that you require to deal with this whole problem?

Sir Chris Wormald: It is difficult for me to comment on what the National Cyber Security Centre is doing. They are building capacity within NHS Digital the entire time.

Rob Shaw: We are. Simon mentioned it at the start, but my staff came in on Friday morning and went home on Monday, unfortunately in the same clothes, pants, socks and so on. That was not a good place to be on that weekend.

Simon Stevens: Too much information.

Rob Shaw: We have around about 18 to 20 deeply technically skilled people. We are doing a graduate scheme, working with local universities, to try to grow our own, but the reality is that these are really sought after skills. A lot of organisations in the private sector can double salaries for

people, and we have lost people through that sort of approach. There are three jobs for every skilled cyber-security expert.

We rely on the fact that people are committed, in terms of their wanting to give something back to the public sector. We have grown a team that realises the difference they make, in terms of the impact on patients and direct care. We are growing that, and we are trying to give them training programmes and to make it so that they have a career ladder and can work through.

However, we will have to continually, across our organisations—not just mine but the local organisations and so on—be able to attract and retain top talent on this. Where we cannot get that, in terms of permanent staff, one thing we have done as a result of WannaCry is to work with the Crown Commercial Service and the National Cyber Security Centre to ask, if they haven't got the staff that have the capability, how they can draw down on trusted suppliers to come in and support them. In the heat of an incident like this, if you bring the wrong supplier in, you can do more harm than good. That is one of the other things we have put on our website—to support local organisations.

Sir Chris Wormald: Nationally, as your question points to, this is an area where the country is short. In my previous life in the Department for Education, that is one of the reasons we added coding so clearly into what schools need to do, because we need to grow more people nationally. The NHS competes in the market for those valuable people with everybody else.

Simon Stevens: Can I make an opportunistic comment that is not directly related to this? It was not a cyber-attack, but there was a Twitter attack on the NHS today. President Trump has tweeted about the national health service today. Unfortunately, respectfully, we suggest that that tweet got the wrong end of the stick, and in fact that people in this country do not want to ditch our NHS, notwithstanding everything we have been talking about today, but they want to keep it and strengthen it.

Our invitation in the NHS, should the President visit later this year, would be for him to spend time with brilliant doctors, hospitals, technology experts and scientists and to hear about the cataract services, the hip replacements, the modern scanners, the world first liver, heart and lung transplant and the genomic revolution, which are all under way here in the NHS. He will go away understanding that healthcare for everybody, delivered at half the cost of the US healthcare system, is something that people in this country are deeply and rightly committed to.

Chair: I am very grateful for that, Mr Stevens. I think we often underestimate our excellent health service. You and others get your fair share of criticism, but you work very hard. I am very grateful to all our witnesses—Sir Chris and your team and Simon Stevens and your team—for coming this afternoon. I thank you very much for all your work during the WannaCry attack. It must have been a worrying time for a few days. Thank you very much for that and for answering our questions this

afternoon.