HOUSE OF LORDS

Revised transcript of evidence taken before

The Select Committee on Digital Skills

Inquiry on

DIGITAL SKILLS

Evidence Session No. 14 *Heard in Public* *Questions 173 - 191*

TUESDAY 28 OCTOBER 2014

10.10 am

Witnesses: Stephanie Daman, Nick Coleman and Hugh Boyes

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Members present

Baroness Morgan of Huyton (Chairman)
Earl of Courtown
Baroness Garden of Frognal
Lord Giddens
Lord Haskel
Lord Holmes of Richmond
Lord Janvrin
Lord Lucas
Lord Macdonald of Tradeston

_____

Examination of Witnesses

Witnesses: **Stephanie Daman**, CEO, Cyber Security Challenge, **Nick Coleman**, Global Head of Security Intelligence, IBM Services, and **Hugh Boyes**, Cyber Security Lead, The Institution of Engineering and Technology

Q173 The Chairman: Thank you for joining us this morning. I will do a bit of a preamble before we start properly. You have a list of interests in front of you, which have been declared by the Committee at previous meetings in July, and they are also in the transcripts. This is a formal evidence-taking session of the Committee and a full shorthand note will be taken. It will be put on the public record in printed form and on the parliamentary website. You will be sent a copy of the transcript and you will be able to revise it in terms of any minor errors. This session is on the record. It is being webcast live and will subsequently be accessible via the parliamentary website. You are very welcome to submit written supplementary evidence after the session. Indeed, if there is something where we are interested in receiving some extra information from you, we will ask you during the session as well. I am reminded to get everybody here to speak up reasonably well so we all hear each other and we get a good recording. That is by way of preamble.

I am going to ask you to introduce yourselves and if you wish to make any opening remarks, please do so. If you do not want to, that is completely fine and we will go straight into the questions. You will find that on some of the questions you may all want to say something, on others you will not, and that is completely fine, so we will just play it by ear as we go along. Ms Daman.

Stephanie Daman: Good morning. I am Stephanie Daman. I am CEO of Cyber Security Challenge UK, which is a small not-for-profit. Our mission is fairly straightforward: it is to get the right number of properly qualified people into the cybersecurity profession. The way we do that is utilise competitions to identify talent and then award job type ready awards to help people get into jobs. So we are talking courses, we are talking things like that. My background is mixed. I had a government background for a long time and then I worked for HSBC in the private sector, so I have both sides of the house.

The Chairman: Thank you very much. Mr Coleman.

Nick Coleman: Good morning. I am Nick Coleman, Global Head of Cyber Security Intelligence services at IBM. I am also an Honorary Professor at Lancaster University and, previous to that, I was with the UK Government as the national reviewer of security and authored the *Coleman Report.*

In terms of what I am going to start with this morning, the challenge of cybersecurity skills is changing; it is a fast-moving market. I think technology is evolving quickly. Therefore, some of the challenges of cloud, of big data analytics, allowing us to do new things in different ways are also creating a challenge for security, so, while we enjoy the benefit, we are doing that. That is a challenge for the citizen and for all of us as we consume services. As I see it, it is a challenge for business and government leaders in having to understand what risk means to their organisation. It is also a challenge of how we get enough information security, professional cybersecurity professionals available to create a vibrant economy in the UK and internationally.

The Chairman: Thank you very much. Mr Boyes.

Hugh Boyes: Good morning. My name is Hugh Boyes. I am the Institution of Engineering and Technology's Cyber Security Lead. I am also a Principal Fellow in the Cyber Security Centre at the University of Warwick. I have a mixed background of both public and private sector, so I have a fairly good understanding of cybersecurity across the board. The work I do with the IET is principally around the skills agenda and spreading knowledge within the engineering and technology base, trying to encourage engineers to understand the cybersecurity issues that affect their jobs.

Q174 The Chairman: Thank you very much. That was a very helpful introduction. Let me start with a bit of an overarching question, which is probably fairly obvious but just to paint the picture for us properly. We have heard from various witnesses in the last few weeks that cybersecurity is terribly important and it is imperative for all of us. It is imperative for all of us as individuals to stay safe. It is also imperative for business to be competitive. Can you just explain for us, in relatively simple terms, why does cybersecurity matter? How significant an issue is it for us and where do you see the gap in the UK at the moment on cybersecurity? Is that increasing or not? Who would like to start? Mr Coleman, shall I start with you?

Nick Coleman: Sure. I think that it is a challenge for all of us. It is a challenge where, if I look at the landscape, in the last few years we have seen more sophisticated, targeted attacks for a different number of motives from a variety of sources. That is principally a concern for our critical assets and protecting them, so that our energy, our banking system and all of our assets continue to run as we would expect them to and do not get disrupted. There is a secondary concern, which is associated with the loss of intellectual property and what our critical assets are and making sure those are protected. What we have seen is an increase; as we have seen an increase in digital, we have also seen an increase in attack.

To put this into perspective, looking at operational data from across the monitoring base that IBM does, we see that mid to large organisations would face about 91 million security events a year. If you think about it in terms of your environment, your house perhaps, it would be 91 million rattles at the door or the window. From that, we have to get down to identifying the 100 or so significant incidents, where—if I take the analogy of your house again—somebody might be in your house or might have taken something from you. We are

getting a lot of data, about 91 million events, down to having to look for the 100 or so things that are critical. When I talk about those cyberattacks, that is what we are talking about.

Therefore, in the context of skills, this is a new threat horizon for some, and some have done a lot of work in critical infrastructure stuff and others are still maturing their approach. Some people are struggling to build their capacity. Again, that comes down a little bit to the users and the people who are both customers and citizens, and all those interfaces, as well as the business and the technical skill.

The Chairman: Thank you. Ms Daman.

Stephanie Daman: Yes, I suppose I would characterise it perhaps a little differently. If you look at our lifestyle these days, everything is based on something that is connected to the internet, whether it is your banking, whether it is paying your tax, whether it is doing your shopping; everything at the bottom has an internet layer. Unless we make sure that that internet layer is properly secure, then none of us is going to have confidence in using it and that will ultimately affect our prosperity, because that way lies prosperity. At the moment, in my view, the real difficulty is that we do not have a sufficient number of properly skilled people to do that protection piece.

The Chairman: Is that because people do not want to go into that part of the business, or is it that the general high-level skills that are needed are so sought by so many people that there are not enough people to go around?

Stephanie Daman: I think it is a mixture of both. That second point is certainly true; there are not enough people with those skills. If you start thinking, "Why are there not enough?" you need to look back into our education system and what we have been doing over the last number of years.

The Chairman: Yes, we have been looking at that.

Q175 Lord Macdonald of Tradeston: Given that risk management is now such a rapidly growing area, and so well rewarded in places like the City, that is surely also true of cybersecurity. The money is there, but are people just very difficult to train? Is it so complex that there is a bottleneck there?

Stephanie Daman: Certainly the money is there and certainly the careers are there. On the face of it, it should be a very popular thing to be doing, but the skills are not there and there is a gap. I call it the lost generation: because we did not teach this specifically in schools, we have a generation of youngsters who went away and taught themselves. If you go away and teach yourself, you do not realise there is a career there. As an organisation, a lot of what we do at the moment is reaching out to try to find those people and trying to persuade them that their future should be within the profession. A lot of them do not have formal qualifications, though, so we are also backfilling on formal qualifications. There is a big gap, but there is no doubt there are good jobs there.

The Chairman: Let me pick up on that a bit further, because it is quite interesting. You take people without formal qualifications, so with-A levels perhaps, or with a different degree altogether.

Stephanie Daman: Our competitions are based around skills in cybersecurity. We do not ask about previous academic qualifications in any way. It is all to do with your skills in this subject, and if we find you are very skilled, we will try to give you the things that you need to

get into the profession. But I think you have raised a very relevant point. A lot of big organisations like to have those formal qualifications—a degree, an A-level—and if you do not have those you do not even get your foot across the door.

The Chairman: Yes. Thank you. Mr Boyes?

Hugh Boyes: Stephanie has mentioned the personal use of the internet and the threats that we face in that space. The area that I am particularly interested in is the whole manufacturing, energy production, transport base, where increasingly that connectivity is used for critical services. If we look at things like the smart grid, smart buildings, these all rely on internet-type technologies. It is not the internet as we know it but it is using the technology, and that commercial technology is fundamentally flawed. It is often very badly configured and the skills for configuring it are quite sophisticated. When we unpack a computer out of the box, it does not come out ready to use as a secure device. It needs hardening if we are to protect it. Those skills need to be taught and it is that problem that we face. We are short of IT-skilled people anyway. IT is often seen as a bit of an accidental career. You may start out doing business studies, engineering, a whole raft of subjects, and then you end up migrating into it. Of course, what we are lacking there is the underpinning knowledge. For example, how does the internet work? What is TCP/IP? How do you secure it?

Q176 Lord Giddens: How much is known about who the cybercriminals and cyberhackers are? Do a significant portion of them have professional qualifications and become rogue agents or are they mainly amateurs? If they are amateurs, I suppose they are more easily outwitted. In reference to the question about the City, is there a grey area where hacking merges with unjustifiable risk, where people are taking risks like they did in the City, which cannot be justified but are not exactly criminal? Is there an analogue to that?

Hugh Boyes: Let me tackle your second question first. Certainly the question of risk is quite an interesting one. Last week, I was briefing a—

Lord Giddens: It is fundamental, is it not?

Hugh Boyes: It is, but it is a case of: how do you get people to understand it? I was working with a team of executives for an SME last week, explaining to them some of the risks. Half an hour into a two-hour session, a number of them were reaching for their phones to turn off apps after we had told them, "Do you realise what that discloses about you, your behaviour, your personal information?" They had not realised that. It is this "free to use", "free to download" and the risk that comes with it. Once we explained the risks to them and they understood what it takes to secure their enterprise, they were saying, "Yes, we need to do that. We need to protect our IPR. We need to protect our communications". But it was that process of taking them through the questions: what are the risks? What are the challenges? Why should you do this? They got the message and they understood it. You asked: who are the cybercriminals? Potentially, cybercrime is extremely lucrative, so it could easily be somebody who is IT trained.

Lord Giddens: It has to be, does it not, if you are really skilled?

Hugh Boyes: Not necessarily. Some of the best hackers are self-taught, so when we look at—

Lord Giddens: No, I mean the rewards you can gain could be gigantic. You can see that.

Hugh Boyes: Exactly. But where you get the talent to create the malware, to do the hacking, it is not necessarily IT professionals. It can be the teenager who decides that that is far more challenging and interesting to them than adopting a normal career.

Lord Giddens: No, I wonder if anyone has done any systematic studies of who they are, or is that not possible? It is also global. You can hack from anywhere. It is not like normal crime at all any more, is it, because of the intensely global nature of everything.

Hugh Boyes: Certainly there are suggestions that in certain countries professionals are being used to target UK assets. That is no secret. The Government says that is an issue, that that is part of the nation state threat to our assets.

Lord Giddens: But would it be true to say that mostly we do not know who they are then?

Hugh Boyes: I suspect the Government knows who they are. I do not personally.

Lord Giddens: No, I meant us organisationally because normally, if you are dealing with criminals, you have some surveys that tell you who they are and where they are located and what their likelihood of committing further crimes is, but when it is global and electronic it would seem to be much more difficult.

Nick Coleman: To some extent, you can look at their homework so that, when you see an attack and when you do the investigation, you can understand some of the skills. Some of them are formally trained and some of them are informally trained. It is a global issue—I think there is no doubt about that—and people are increasingly skilled in different ways. There are different groups who have different motivations and some of those skills will be attractive to different groups in different ways. You certainly can see a maturity of the skills in that I think, if we go back five years, people were trying things in their bedrooms and that seemed to be the exciting stuff. This has matured on to where we are talking about a targeted situation, a criminal issue, and these people are relatively well organised now. They almost have businesses with a common structure. They have people who look after HR. They have people who look after finance. These are properly run organisations in some respects, so much more sophisticated.

Stephanie Daman: I think law enforcement has some idea of where these groups are and how they operate. But, like everybody else, law enforcement is suffering because they cannot recruit properly skilled people with the matching skills to bring some of these networks down. There is some knowledge but actually moving that to deal with it is more difficult.

The Chairman: The capability, yes.

Q177 Lord Haskel: We are interested in the digital skills of the population as a whole. Are you satisfied that, when digital skills are being taught, people are made aware of all of these things that we are discussing at the moment? Would you think that that is an important part of teaching digital skills to the population as a whole?

Hugh Boyes: With digital skills, and certainly with cyberskills, we need to be quite clear that there are different layers of skills. At a personal level, we all need some of those skills. We need to be aware of how to be safe online; we need to understand what risky behaviour is.

Lord Haskel: Is it being taught at the moment?

Hugh Boyes: Schools are trying, but you have to remember that an awfully large percentage of the population is outside the school system; they are outside formal education and they are often not aware of the threats that the new technology brings with it. When you then move into people in their working lives, we see regularly events where their behaviour online and their behaviour using their corporate IT puts them at risk. That is a space where, effectively, businesses and employers need to look at providing the education and training.

Stephanie Daman: I think it is very patchy in the schools, and I think a lot of that is down to teachers not knowing what and how to teach. There is a huge need to rectify that, otherwise we are going to have patches where digital skills teaching is very good and other patches where it is very poor.

The Chairman: We had a very long session on teaching last week and it was absolutely clear it was very patchy.

Q178 Baroness Garden of Frognal: I think you have answered quite a lot of the questions I was going to ask you about the cybersecurity skills shortfall. Just continuing on this theme of what is taught at school, we are aware that there is a new computing and digital syllabus now being introduced. Would you consider that the aspects of cybersecurity should be a key part of that syllabus when it is being taught, and generally are universities preparing young people, if it is universities where the shortfall is needed? Ms Daman, I was interested in what you were saying about your skills competition where you are not looking for specific qualifications but are trying to assess the skills without that. How do we move that aspect forward?

Stephanie Daman: Certainly within the schools there is a curriculum. To my mind—and I suspect to my colleagues' minds too—it is absolutely vital that cybersecurity is covered in the right sort of way. I also agree with my colleague, Hugh, that there are different layers of skills. In my view, one thing that is happening is that we are beginning to teach safety at the lower levels and we are beginning to teach cyber at the higher levels, but I think we are perhaps missing some of the linkages in between. We understand there is a difference between safety and cybersecurity, but I am not sure whether schools understand that nuance.

Baroness Garden of Frognal: Yes, there is a big movement for safety online, to try to make sure that children are aware of cyberbullying and those aspects of things.

Stephanie Daman: Yes, there is.

Baroness Garden of Frognal: But you are saying it is not then a seamless curve up to the more sophisticated levels.

Stephanie Daman: Exactly that. There is not a seamless curve and increasingly, from my knowledge and from our own schools' programme, which we have within the Challenge, I feel that this is a missing link. We are not being very helpful to the schools by making that particular division. Although we understand what it is, I am not sure it is very helpful for the schools, because that just confuses the issue. But, yes, it is absolutely vital that it should be taught at those levels.

Hugh Boyes: If we are looking at the teaching outside of schools—so in FE and HE colleges—one of the big gaps is the way we teach coding, so a fundamental part of cybersecurity is the quality of the software we write. The Government has been investing some money in a thing

called the Trustworthy Software Initiative, and we are trying to make progress in injecting core skills, core knowledge into university curriculums, but it is quite slow progress because it is quite hard work.

The Chairman: At the moment, it tends to be an add-on rather than integral to the course?

Hugh Boyes: Yes. Certainly from the IET's perspective, we would like to make that integral. We are keen to encourage any accredited degrees—whether we accredit them or the BCS accredits them—to deal with the question of good-quality coding, not just teaching them how to code, but how to defensively code, because that will reduce our risk.

Nick Coleman: If you have teenagers or you are trying to do it at primary school, of course they are busy talking to their fellow friends and understanding and getting ahead of the technology often of the teachers and of the parents. This is not just a challenge at school; it is also about the whole environment and where you get those skills. That comes down to the adult population as well. So I do not think it is just in schools; it is a society challenge and I think we have to make it very practical. For me it is how we use services. You log on to a banking service or an electricity provider online, or you are going to get a smart meter, and if it comes as part of that education and part of you using the service I think it is very powerful. If we have it as an add-on later it is very, very difficult. We still have to do that education, but I think we missed—

The Chairman: It is sort of boring, yes.

Nick Coleman: It comes with the car, it comes with the service and you get it as part of your life. I think that is where we have to move to.

The Chairman: That is very interesting.

Q179 Lord Lucas: Karen Price of e-skills said to us, when she gave evidence, that she was concerned that we were very bad at bringing returners and career changers into tech occupations. I see you have some very interesting competitions and a MOOC on your site. What is out there that would enable someone, say, who has a career as a nurse—and, therefore, is pretty careful and exact in what they do and is the sort of person who will pick up the faulty software in the example you give on your site—to click on to the idea, "Maybe I can make this conversion"? Then what course do they do afterwards that industry will regard as serious enough that they would take the risk of picking up that person and training them? Is there that route and can it be created for adult returners and career changers?

Stephanie Daman: I do not think there is an obvious route. There are ways of doing it. I suppose I would say this but we have some people who have no background in this subject at all who start playing our competitions because they are interested in playing competitions. I have one person particularly in mind who started with us about a year ago. He was very interested in the subject and started playing the competitions. He did well, moved through the competitions and ended up at our finale at the end of the year. He was immediately picked up by a number of employers who could see he was very skilled. He had that great mix of good technical skills but also that ability to translate that into business risk language. He is now in a cybersecurity job with a large bank. That is a perfect example of somebody who came to it not because they had qualifications; they came to it and transitioned. In many respects, it is career transitioners who will save our skill shortage because, much as we want a pipeline, you have to have people who are going to transfer now. For example, we have been doing work around people coming out of the armed forces,

taking the skills that they have, which are huge, and moving into this space. But certainly I am not aware of an obvious pathway. There is not one.

Nick Coleman: There is certainly an MSc in cybersecurity and there are now four Government-recognised centres of excellence who are teaching MScs in the UK for universities. We are starting to see people who have, for example, a scientific background—perhaps in biology or chemistry or something like that—looking at cyber because it is popular and then using the master's level as a route in. That is a recognised entry level into a more professional or advanced layer into an organisation. Of course, we have the challenge of getting the right graduates who are STEM ready and cybersecurity ready. We also have a challenge at the professional advanced layer, where frankly we do not have enough people there either. This route with the master's level starts to form someone quite well with a discipline, which helps.

The Chairman: Mr Boyes, I do not know whether you have anything, do you?

Hugh Boyes: Just picking up on what Stephanie was saying about the skill sets, one of the interesting challenges with cybersecurity is not just about technology. There are significant people and process aspects, so this is about being able to communicate how to behave, how to improve your system design. It is an area that we often overlook. We think of cybersecurity as being deeply technical, whereas it is quite a broad subject.

Q180 Lord Macdonald of Tradeston: Building on this, I see here that last year the National Audit Office reported that it would take the UK 20 years to close the cyberskills gap. Given the almost existential risk, which you alluded to in terms of a critical national infrastructure, we cannot wait 20 years. Is there some emergency task force way of pushing this through and getting a quicker, perhaps even dirtier, solution rather than waiting for 20 years for the educational system to slowly deliver the talent?

Nick Coleman: I think we have to do both, in some respects. We have to build the set of skills, through competitions, through university education. I am also involved in getting it involved in MBA programmes, so starting to get it on business degrees, taught in business language, so we are starting to broaden that pool of people. In parallel we are moving to new models that will address some of it, such as cloud computing, where you will be able get in to and access infrastructures that have security designed in that have some of those controls. One law firm said to me that previously they had one person in their IT department and they had no idea what they were doing. They moved to the cloud and that gave them standard operating procedures, it gave them a whole level of cyberskills that they could not have accessed on their own. I think it is partly the skills and partly the technology evolution that will help.

Stephanie Daman: I think it is also innovation: being innovative, stepping outside the box. We have apprenticeships starting, we have new training courses, and we have competitions. I think we need a variety of different ways to encourage people to get into this subject. We do not need to throw out all the old ways of doing things, because that would be very foolish and quite unnecessary, but I think we need to accept that this is a subject where the old ways of doing things do not necessarily work. I am coming back slightly to the HR expectation of formal qualification or university degrees. If we want people with the skills, we have to accept that they are not all going to look like that and we have to accommodate that.

Hugh Boyes: If we are looking at innovation, we need to look quite closely at what was achieved in health and safety. Over the last 20 to 30 years, we have seen a culture shift in the UK. Now if you go into any engineering organisation, safety is high on the agenda. It is often the first item on a meeting agenda. We need to transition security to that status, where everybody in an organisation is doing it. It is not just for the specialists.

The Chairman: That is very good. We will bank that, because we will ask you at the end to give us one idea. That is exactly the sort of bankable specific that is very helpful to us.

Q181 Lord Giddens: Could I go back to the issue of risks and dangers and how we deal with them, since that is the core of it? I am an economist primarily and if you look at the nature of the global economy, it has changed in the most unbelievable way over the past 20 years. It has been calculated that, if you look at the proportion of cash in the economy, it is 100 times less than it was 20 years ago, so physical cash has dwindled away. When you had cash, you had an independent way of assessing things. You can pass money on as an independent existence; now money is just dots in computers. So, if I shift a dot in your bank account three places, you become a millionaire; I shift it four places, you become a billionaire. How vulnerable is this new electronic economy either to attack or to systemic risk? Having looked at it quite a lot myself, it seems to me it is intrinsically quite vulnerable and, since it has never existed before, it is like a new frontier here.

Then you may have answered the second question but, in everyday life, how do you deal with the proliferation of scams that exist? I counted up the number of passwords I have—and I am sure it applies to most people in the room—and I have 30 passwords. If you include the ones you have to get money out of the wall in the bank or you have to get in to the Houses of Parliament and so on, how are you going to handle this on an individual level? You can get an electronic vault and you can put them in there but, if someone gets the master password to that electronic vault, you are presumably lost. That seems to me a really serious issue on the level of everyday life: how you manage your own personal security in relation to these risks. It would be good if you could comment on these two aspects of it all, because they seem to me to be where the core issues are. Obviously we need to train people to deal with them, but they seem to me pretty new. I do not think they existed in this way before.

Nick Coleman: Talking about digital currencies as an example, what we have seen, as new models of bitcoins and other forms of digital cash, the number of attacks on those infrastructures and trying to steal bitcoins and exploit them is growing significantly—

Lord Giddens: Well, this guy lost about £800 million or something.

Nick Coleman: Also you have seen recently high-profile credit card attacks of retailers, not of banks. They are going after the retailers and where they are stored. There is no doubt that, as we have gone to digital, we have that. I think the skill set that we need, though, is that we need people with practical experience and understanding of the risk and how to manage that risk, and understanding how technology is changing. Therefore, if these people do not have an understanding of that environment, it is very difficult. In reality, we are not going to prevent every attack. So, as an industry, we have had to focus more on response and intelligence, to be able to spot and then monitor the environment, as well as design. A little bit is in designing the infrastructure and getting the skills of architects, which we have not talked about, so it is about a lot of other related industries and IT professionals building it in securely, the coding that Mr Boyes talked about, all those things, but also about getting

people—and this is a big growth industry—who understand how to operate intelligence centres and the intelligence response.

Q182 The Chairman: I have a second point about the individual level. We have talked about there being a little bit in schools, but it is pretty patchy and it is not joined up properly. Where do any of us, or anybody else out on the street, go to think, "I have made my own personal use of the internet as secure as it can be"? Where is the kitemark on that?

Lord Giddens: It is 60 passwords.

The Chairman: Yes, exactly. It is not going to be the citizens advice bureau, so where is it that you go that says, "Here you are. Realistically, this is the best we have at the moment"?

Nick Coleman: As we have talked about, it is patchy right now. I think where one is going to go is to one's internet provider, to one's electricity provider, to one's bank and, as you can see, to one's Government. When you consume those services I think that is where you will say, "Hang on. What do I need to log in? Hang on, what is the password?" I think that is the first level, but we are also going to have to think about a second level, be they cybersecurity professionals, which people can have in their communities and you can have in your networks, in everybody's networks—somebody they can turn to and trust. That is where the institutions, the professional bodies, are trying to certify people to recognised professional standards. I have been through some of it myself. I think that gives us some kitemark. I do not think you can do the kitemark for your environment or for your computer at any point, but I think you can have a kitemark as to whether somebody knows what they are talking about and has been tested both on skills and experience.

Stephanie Daman: Also the Government has created several initiatives to try to attack this particular issue: Get Safe Online, Cyber Streetwise. I think there is a question around why those perhaps do not receive the attention that you might hope they do. I am reminded of Clunk Click Every Trip, which was in everybody's consciousness.

The Chairman: Yes. I have to say, I have never heard of the ones you have just referred to.

Stephanie Daman: I suspect that illustrates why they have not been successful, which is a pity because they have exactly this sort of information: how you do things, how you can make yourself safe. Perhaps there is an issue around how we do that general awareness campaign, because Clunk Click Every Trip was very successful.

Q183 Lord Giddens: If I might say something, I also think one should not just succumb to the electronic world. I think sometimes people should be encouraged to use back-to-the-future solutions. If you keep things written down and you lock them away, they are more secure probably than they are online. Even organisations might have to go back to doing things they used to do in the past and having independent verification. I do not think it all has to be electronic on the level of personal life. It at least takes you out of the system for a bit. You have to make sure that no one gets into your safe, though, or into your locked drawer, very likely.

Stephanie Daman: Yes, absolutely. It does not all need to be electronic. I am also minded that in this particular space the technology has moved so quickly that all of those protective things have not caught up. To me there always seems to be a gap between that: the technology develops, it does amazing things, but everyone forgets that there is a flipside to that and that flipside takes a long time to catch up.

Q184 Lord Janvrin: If I can follow up on this point, and it is almost a philosophical point: is there an ebb and flow between offence and defence in this whole area? It is like the First World War, when the heavy machine gun was defence, and someone came along and said "tank" and offence was dominant for a bit. Are you seeing the same? In terms of technological change, are we seeing the same kind of ebb and flow between the hacker technological change and the defensive technological change, or is that too simplistic?

Stephanie Daman: My own view is that, yes, we are. I think the trouble with this particular subject is that hackers have no boundaries. We do. A hacker can do anything they like online and they do not have any ethics to guide them. That keeps them well ahead, because they will conceive of and do things that we would not even dream of doing. We are then fighting to find defensive measures to tackle those things.

Lord Janvrin: So they can use chemical weapons and the rest of us cannot. Sorry, I am in World War I mode, but—

Stephanie Daman: Yes, it is exactly the same as terrorism in many respects. A terrorist will do things we would not even dream of, so how do you protect against something that you cannot conceive of? It is the same issue.

Nick Coleman: I do not think it is all new, though. This concept makes it sound like everything just appeared last year. The reality is some of the attacks that happened have been known-about vulnerabilities, sometimes for 10 years. From the outside perspective, if you leave your house vulnerable an attacker will look at you and go, "Oh, you might be easy". Whereas if you use good locks and they have a look, you become known as quite a hard organisation and they might go next door because it is easier. I think in your ebb and flow defence certainly alters the landscape, there is no doubt about it, although there is a reality that if you just rely on "design it", there are new techniques coming along as well that mean that you have to be able to spot it, so it does have to be this ebb and flow of understanding and responding.

Hugh Boyes: As we heard earlier, part of the challenge is the scale of the attacks on organisations. What we are facing is almost a tsunami of electronic attacks. It just requires one to get through successfully and a system is compromised.

The Chairman: And it destroys confidence.

Hugh Boyes: Yes, and this is a very difficult balance because you can repel 99.99%, but it is the one bit of malware that gets inside the fence that breaks down your boundaries. The innovation we are seeing in some of the attacks is quite interesting. At times they are actually turning our own technology against us, so that—

Lord Giddens: If I may say so, that is a very good point, which the Committee should register, because that is the nature of system risk. We saw what happened in the global financial crisis. It could not have happened like that before the economy became electronic, so you only need one system risk that you fail to grip and then the war analogy holds. It seems to me that you could have various kinds of catastrophes, depending on what systems are involved.

Nick Coleman: If you look at the recent significant attacks, then they all become a leadership issue. Part of the reason why I talked about getting this into business schools is that all the CEOs of these companies and organisations—public or private sector—have had to stand up and explain some quite technical attacks and what it meant in the business, not trying to

confuse the people and their stakeholders and saying, “Well, it is this geeky piece here”. Real leadership comes down to risk management, so whether we talk about your school and the people and the pupils in that school, whether we talk about Parliament, whether we talk about public sector organisations, it has now translated where we need the professional skills, but we need the leadership skills to be able to understand the risk that they are taking and what they want to invest in.

The Chairman: Yes, that is very clear.

Q185 Lord Lucas: You seek to put the onus on us to be secure, but you do not provide us with the systems to do it. You provide immense amounts of conflicting advice. As Lord Giddens said, you end up with 30 passwords, you do not remember them, and then you make us change so we forget them again. If we die, who is going to make sense of anything? Surely you must get your heads together and produce something like Clunk Click that we can do. Would it not be safe if we wrote our passwords down and kept them somewhere at home? What is the danger in that? Can you do something that is doable and then produce consistent advice that stays there, so that then we might learn to do it?

Hugh Boyes: In a sense, yes, you can write passwords down. This is where we get conflicting advice. In a business environment, the reason why we say, “Do not write passwords down” is often they are written down, put on a Post-it and left by the computer. For critical passwords, what is wrong with storing them securely at home? That is one of the ways—

Lord Lucas: Yes, but that is not in any advice anywhere.

Hugh Boyes: Quite.

Lord Lucas: If you want Clunk Click, you have to produce that simple thing that we can just do.

Hugh Boyes: Some of the things that we see, which are supposed to be there to make life easier—for example, the federated access through things like Facebook, Yahoo or Google—actually increase the risk. If that particular account of yours gets hacked, it then gives access to all the accounts that are linked to it. It is often not spelt out to the public that you are trading their convenience and speed for a different risk.

Nick Coleman: I think there is good news—and I would like to give a little bit of good news—that we are moving to a world where technology is also going to help us understand what normal looks like in our environment, so imagine you have a phone, a tablet or whatever. We can now start to look for things to understand when the behaviour on that device is normal. In other words, if you open a document and it starts to do other things, you have a problem. We have to get new solutions. By the way, part of the skills discussion is not just about getting skills in organisations. I think we have to have a vibrant cybersecurity market in the UK. If we do not have those professionals, we are not going to get the start-up environments powered up to create the next generation of solutions. We are already seeing some approaches that are going to help in simplifying by designing it into processes and hopefully simplify the 30 password problem, which I am sure we all wrestle with.

Q186 The Chairman: Is there a trust issue? Let me can take you back to the analogy you used. We have all been told over the years to secure our houses, in a sense, and we have received pretty consistent advice on that. Ultimately, if we were broken into, then probably somebody will come around from the police and give advice or whatever. There is a body of

people where you think, “That is probably reasonable advice,” and they are not necessarily trying to flog you something at the same time. But on the issue of whether we write our passwords down on a piece of paper and keep them in a locked drawer, is there a danger that we are told we have to buy the next thing to protect our passwords, the next app or the next whatever it is, but at the same time you feel as you are doing that, “I am buying that” or, “Somebody is making money out of me doing this”? As consumers and as citizens, where do we go to get what we consider is unbiased advice that builds our confidence in the internet and the structures we need to be competitive?

Stephanie Daman: You would hope that the place was government. You would hope that this was a public interest thing, but I think we are almost going into a cultural change. In the years of Clunk Click, if there was a government message that came out on the television that said, “You had to put your seatbelt on”, I think mostly the tendency was to accept that and do it. I am not so sure that that exists today. It is not for me to try to understand why that is the case, but it seems to me that it might be the reason why things like Cyber Streetwise and Get Safe Online are not so widely known about and accepted. I think there is partly a trust issue and I am sure that is part of it, but I think my question would be: that advice is available but why is it that it is so difficult to find it? Why is it that people do not know about it? What is it that we have missed? How have we failed to get the word out there, because we do seem to have done?

The Chairman: We had better move on. Thank you very much. Where are we up to? Lord Janvrin.

Q187 Lord Janvrin: It is almost a continuation of this, but taking it to the corporate or SME level, how do they get advice in looking at their own protection? Is there some way in which this could be clustered? In other words, you would have regional cyber experts who would be available for SMEs to tap into to seek knowledge and to seek solutions. We have been talking at the individual citizen level. At the SME level, can you see how they can get this kind of advice?

Stephanie Daman: There is a very good example of that with the Malvern cluster, which provides a great deal of that. The Government has also produced something called Cyber Essentials, which is also aimed at SMEs, and that is exactly what it sounds like. It is the essential things that an SME needs to know to protect themselves. There are initiatives out there to tackle these things, and my strong feeling particularly is that we are not marketing these; we are not getting the word out sufficiently, because the material is there.

Nick Coleman: I think there are two levels of this. There is the level where you want to get a general awareness and you want to look at a website or you want to try to find out some information and you want to try to figure out what you do with your passwords and that kind of stuff. Then there is another level, which is where you are designing—you might be a relatively small organisation but you might be a supplier of a large organisation, so you might be connected in. You might be a small organisation but be in the financial services industry and have quite a big footprint, but you do not have many employees. Then it comes down to getting professional advice. There is a marketplace and that is where we need the skills in the UK to make sure it is a vibrant marketplace to give that professional advice; it is a commercial marketplace.

Then I think the other thing is there are increasing ways of delivering this, not just via advice, but via services, so buying in the next generation of services and understanding what is right for your business. I think the good news is with the growing publicity around the challenge, which means that a lot of business leaders are looking. As I say, the stuff I am doing is to talk to them in business terms, not in technical terms, so they start to get it as a risk. Because they understand other risks, it is just making business and public sector leaders understand this as a risk decision. So that, where the board members can start asking some of the questions in risk terms; and can tell whether they have the in-house skills to be able to give them the answer or whether they need to go out. In some cases, I have heard them say, "I am not getting it from my own organisation", so we need to build our own capability and get external help to support.

Hugh Boyes: We have just touched on Cyber Essentials, which is a scheme that is very much aimed at SMEs. The challenge is that, if you go beyond the basic step of self-analysis and self-check, delivering that sort of advice is not cheap. You are looking at a professional whose costs and income potentially are similar to those of solicitors, accountants and so on. When you start looking at SMEs, they have to go to an accountant to have their accounts done. That is a legal requirement. They do not have to buy IT security advice and cybersecurity advice, so they decide not to. Unless we can find some way of getting that advice to them at an affordable price, they will not take it.

Q188 Lord Macdonald of Tradeston: On this question of how important it is to have a much higher profile for this issue, where in government do you think such a campaign should be directed from? Is it from the Cabinet Office or do you just leave it to the individual departments, whether it is BIS or the Ministry of Defence? I am sure the security departments are active in their critical national infrastructure, but there does not seem to be somebody whose voice the nation is impelled to listen to when it comes to digital security, despite its obvious importance.

Stephanie Daman: It could emanate from several different departments, but the Cabinet Office seems to me to be currently in the lead, so I would favour the Cabinet Office, simply because they already have a number of these pieces in place. I have often wondered whether what we are lacking is some sort of champion, some recognised person that everyone respects who could give out these messages. We do not have that sort of person on this subject and I think we suffer for that.

Hugh Boyes: I think Government needs to use all of its levers. It should not be down to a single department like the Cabinet Office or BIS. We need to make sure that we are using the influence we have across the whole of government, so Ofgem should be dealing with the energy industry. The regulators have incredible power; they can mandate. If we are looking at education, we need DfE fully engaged. It is no good leaving it to BIS and saying it is a workplace issue. My position would be that this is not for a single department. It is for the whole of government to energise and use.

Nick Coleman: I served in the Cabinet Office and wrote the *Coleman Report* from there, which talked about government departments having a role in security. That was about delivery of public services and citizens' services and running the function of government, so I think the Cabinet Office clearly has a cross-cutting role, but then departments have a role, as I have reflected.

The other thing is that we have to start to have the discussion about enabling the good things that are happening in government, so the stuff that is happening in skills, in GCHQ and, again, programmes such as the recognition of a master's. I think we should probably be making a bigger noise about that, because we have probably have not raised it as much as we could in industry. As my colleagues have said, there are multiple bits of government and government obviously needs to look after itself. BIS can help with the outreach to business and the industry.

Fundamentally, on skills, it is about the national framework that the Government has started to put in place for itself and has done some good work on, but it is also a role that it has played in promoting good work, which I think both in the UK and internationally can show that we can grow a pipeline of people and get some talent, here and internationally, coming to learn cyber. I think the more people we can have embedded into those skills, if we promote the services that are running, the more we will increase the flow and I think that is certainly what Government could really help with.

Lord Macdonald of Tradeston: From your background in government, Mr Coleman, is there a sense there, do you think, in the Cabinet Office perhaps, of not being too alarmist and keeping this thing a bit under the radar, so that you are working with a lot of the key industries but you do not want to frighten the horses outside?

Nick Coleman: I do not think so. My report is there, which sets out both the challenge and the recommendations for dealing with it. I think it has to be a balance of enjoying new ways of doing work and new ways of flexibility, but at the same time we have to understand the risk. I think that the Government probably has it about right. I think if it made it over-sensationalised it would turn a lot of people off, and so you have to have a balance. I then think you have to build the capability behind. For example, the Government has senior information risk owners—I talked about having department-level board representatives who would not necessarily be cyber people or IT people, but would be the champion—who have made a big difference. Some of the things have put it into quite a lot of context and then you can turn around to other sectors and local government and say, "Are you doing the same things? Do you have somebody at your board who understands this? Are you really?" I think overall it is about right, but it is growing and we are going to have to keep talking about it being the reality.

Q189 Lord Holmes of Richmond: Good morning. You have touched on a number of issues around this. I want to develop the points around inclusion and inequality. We have heard a lot of evidence about how the digital revolution will increase inequalities, and obviously the areas of safety, security and privacy online come into that. What do you think is the best way to inform everybody around protecting their privacy and having safety online and at what age do you think they should begin?

Stephanie Daman: I think it needs to start at school. It needs to start in primary school and it needs to be in every single school, not just patchily across the UK.

Hugh Boyes: In a sense, I think I have missed a trick in trying to communicate cybersecurity. We have had these initiatives to get the digitally excluded online. For example, I am aware of foster parents who have been given computers. They are just given the computer and they are not given any training with it. That was an ideal time, when they were given the machine for the first time, to educate them as to how to be safe online and how to protect their

charges. Looking ahead, I think that is an area where if we are rolling out more of these inclusion programmes, we need to build the training and the skills element into the rollout of the hardware or the access.

Nick Coleman: I think it has to come earlier, when you get your first mobile phone. I am seeing lots of people, eight, nine years old, getting their phones and I think then we start to have the challenge of: do the parents know what they are doing with it? Do they understand? It is the age there. I think similarly it is also in all the games that they play and the social networks. It allows us a real opportunity—both in schools but also more widely—to get to them in those environments. That is what they are up to, so if we embed it into those things, I think we have a chance.

Lord Holmes of Richmond: On the practicality of rolling that out and enabling that to happen, do you think there is a philosophical hurdle to be got over from people who are currently in the industry, in terms of the sense of the internet being unregulated, free, with Yahoo, go to the frontier, all that stuff? Though obviously you panellists understand this very clearly and it is a critical and important business, is there a sense for a lot of people that this runs counter to that free spirit?

Stephanie Daman: Yes, I think there is. I think that is our own fault. Again, back to schools, one of the things that I notice with a lot of the candidates I see who are self-taught is that they are very, very woolly about ethics; they are very woolly about what is acceptable and what is not. That is simply because they have not been taught what is acceptable and what is not.

The Chairman: Yes, that is very interesting. Anybody else want to come in on this? No, that is fine.

Q190 Lord Giddens: On the big issues around terrorism in everyday life for children, what trolls do to people and cyberbullying and so on, they fall within the general category of security of the individual, I would have thought. How are we going to deal with those, because it cannot just be a matter of individual training, can it? There has to be some systemic intervention of some sort. You cannot have absolute freedom to say anything to anybody because then you can terrorise them. A troll might find out where you live, might say, "I know the names of your children and I am going to come around and burn your house down". You might know one of those children. I am not clear in my own mind, and perhaps it is not your field but it seems to me to be part of cybersecurity.

The Chairman: It is part of law enforcement.

Lord Giddens: Yes. You just leave it to the police, is that the answer?

Hugh Boyes: I think what you are looking at in some ways is a cultural shift. In personal behaviour, face to face, there are accepted cultural norms. In cyberspace, there are few. We need to start developing those norms so that children understand that cyberbullying is not acceptable. But that is a large issue for society. You cannot just teach it; you have to get people to believe it, behave it. We also need, for example, legislation to be used sensibly. When we saw the cybernats and their behaviour in the recent referendum, it was outrageous. That should not be tolerated. That is not what we should accept in our society, but how do you deal with it? It is almost treated as though it does not matter, but if we encourage people to believe that and to behave that way, it will get worse, so we need to find ways of stopping that.

Lord Giddens: But all these things to me are compounded by the fact that government is national and you are dealing with a truly global phenomenon, which a national Government can only very partially control.

The Chairman: I am going to pause on this, because I think we could go on for an hour on this. Can we go on to the last question, Lord Courtown?

Q191 Earl of Courtown: This is a question that we have asked all our panellists, and just remembering why we are here and the whole point of this Committee: we would like to make recommendations to Government to improve UK competitiveness in respect of digital skills. What is your one point, bearing in mind financial ability to deliver? What is the one point that you would like to suggest that we could recommend?

Hugh Boyes: I would like to see greater encouragement of people to take up training in this area, or training generally in technology skills. At present, the way our tax system works, training cannot be set against tax, either at personal level or often at a company level. We need to ensure that we are upskilling our workforce. Technology is moving fast and the Government could do various things to encourage employers and the individual to raise their skill levels through formal and informal training.

Nick Coleman: I think for me the one thing we can do is make the university system much more relevant, as in: continue that journey to make it a fast-moving response to emerging technology. If I think five years back we were hardly talking about cloud. Now if you are leaving university without an understanding of cloud, how are you relevant? Also, we see a lot of graduates where, frankly, soft skills—not just the formal education but the way of responding and fitting into employment—would be helpful. I do not think it will cost very much and I think we do a lot of it in a lot of places already, but we should make sure that the curriculum on those master's degrees and those undergraduate degrees, both in computing and the specialist degrees, is focused on keeping track of where the technology is, so it is experiential learning rather than all applied.

Stephanie Daman: I would say, "Get it right in the schools, because that is the fundamental thing". If you give the teachers the resources they need to teach this properly at that level, you serve two purposes. You serve the wider digital skills agenda, but you also build that pool of people who I want coming out the other end, who I can upskill into the cybersecurity profession. With that one thing, I think you would serve two purposes.

The Chairman: Thank you very much indeed. That was really useful, thank you.