HOUSE OF LORDS

Select Committee on Risk Assessment and Risk Planning

Corrected oral evidence: Risk assessment and risk planning

Wednesday 17 March 2021

10.15 am

Watch the meeting

Members present: Lord Arbuthnot of Edrom (The Chair); Lord Browne of Ladyton; Lord Clement-Jones; Lord Mair; Baroness McGregor-Smith; Lord O'Shaughnessy; Lord Rees of Ludlow; Lord Robertson of Port Ellen; Baroness Symons of Vernham; Viscount Thurso; Lord Triesman.

Evidence Session No. 14 Virtual Proceeding Questions 147 - 154

Witnesses

I: Lindsey Fussell, Group Director for Networks and Communications, Ofcom; Cathryn Scott, Director, Enforcement and Emerging Issues, Ofgem; Chris Train OBE, Former CEO, Cadent.

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.

3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witnesses

Lindsey Fussell, Cathryn Scott and Chris Train OBE.

Q147 **The Chair:** Good morning and welcome to this evidence session of the Lords Select Committee on Risk Assessment and Risk Planning. We are hearing this morning from the regulators and from a panel of experts on resilience. Welcome to our witnesses. Afterwards, you will have the opportunity to correct the transcript that will be taken if that should be necessary.

We have two panels. The first panel consists of Lindsey Fussell, the group director for networks and communications at Ofcom, Cathryn Scott, the director for enforcement and emerging issues at Ofgem, and Chris Train OBE, the former chief executive officer at Cadent. Please do not feel it is necessary for each member of each panel to answer every question. The first question I have is directed to the regulators, Lindsey Fussell and Cathryn Scott. Could you please give us an overview of what mechanisms you use to ensure resilience and security in the sectors you regulate?

Lindsey Fussell: Good morning and thank you for inviting me. In the telecom sector, which is the sector I am concerned with, policy on security and resilience is set by the Government through DCMS. In practice, that means the Communications Act places obligations directly on operators, on telecoms companies themselves, to ensure the security and resilience of their systems, and then gives Ofcom the power to monitor and enforce compliance against those obligations. We do that in a number of ways: first, by setting best practice for those companies and publishing guidance; secondly, by monitoring the incidents they report to us and trying to learn lessons; and, thirdly, where necessary opening investigations and enforcing.

It might be worth me mentioning now that those provisions are proposed to be changed by some legislation, the Telecommunications (Security) Bill, which I think is currently just coming up to Report stage at the Commons before it comes to the House of Lords. It places far more prescriptive obligations on operators relating to telecoms security and strengthens our enforcement, compliance and monitoring powers.

Separately, we also have some responsibility under the network security and information directive for certain kinds of digital infrastructure providers. We have powers to monitor their compliance against the obligations that are put on them.

Cathryn Scott: In the energy sector, as with telecoms, the Government have overall responsibility for ensuring resilience. As the regulator, we have a role in ensuring the regulated companies are set up to deliver on that. It is worth noting at the outset that there are different categories of resilience-related risks that we are alive to in Ofgem and make provision for. The first is the cybersecurity threats, which I know you are interested in. The second is general security of supply risks, which include day-to-day and sometimes minute-to-minute system-balancing issues and network resilience. The third is about ensuring the financial health of

network companies and suppliers to make sure they can provide the services they do.

I can cover each of the mechanisms we use, because they are slightly different in these different areas, and then I can provide any more details if you want. On cyber, prior to 2018 our main mechanism for ensuring resilience in cybersecurity was by funding through our network price controls. Companies would submit a request for funding cyber improvements, generally through their IT business plans, which were reviewed through a value-for-money lens, as there was no cyber-specific regulatory framework in place.

Since 2018, we have been the competent authority, jointly with BEIS, under the network and information systems regulations—NIS—for downstream gas and electricity. We are responsible under NIS for ensuring that operators of essential services, which are basically the network companies and large power stations, comply with their duties to take appropriate and proportionate measures to manage and help to prevent or mitigate the risk. We do that through many different actions, which I can go into in more detail if you like.

On the other risks, we have a number of mechanisms to support security of supply and network resilience, for example. We have powers to impose obligations on the system operator and network companies, requiring them to comply with certain security standards—for example, how much back-up power should be held in reserve every day and the processes they need to follow in the event of a major power cut. In the case of non-compliance with these obligations, we can also enforce. Fortunately, because of the fact that the UK has one of the most reliable systems in the world, we do not often have to take enforcement action.

Through our price controls, we also ensure the system operator and the network companies have sufficient funding to invest in resilient infrastructure. We also provide regulatory support for some of the resilience tools that have been established by government. For example, we monitor the effectiveness of the capacity market, which secures investment in reliable capacity to make sure there is sufficient generation available in the system. I will stop there, but I am happy to go into more detail if needed.

The Chair: You talk about security of supply. In view of what you said about the network, does that include security of distribution?

Cathryn Scott: If things happen on the distribution network, it can have impacts on consumers who are customers on that distribution network. It can also have a knock-on effect in relation to the transmission network. We are concerned about those issues, yes.

The Chair: Could you both consider, please, how cyber risks compare with other risks, in their profile, their likelihood, their severity and our vulnerability to those risks?

Cathryn Scott: Cybersecurity is a growing and evolving threat worldwide. The move to a smarter, more connected and more flexible energy system that is more digitised will present new threats and challenges to our energy system. Given this, cyber resilience is treated as a key Ofgem strategic risk. The risk is reviewed by our board, as are the actions we are taking to try to manage the risk and encourage operators of essential services to manage those risks.

It is not necessarily helpful to compare and contrast different risks, as we think each of them is really important in a different way. Ultimately, we are concerned about maintaining a secure energy system, so that customers do not experience blackouts and the resilience is provided in the most efficient and effective way, so that consumers do not have to pay an unfair price.

Lindsey Fussell: This is not a very straightforward picture. The first thing to recognise is that every company and organisation in the UK—I am sure the House of Lords is no different in this, for example—suffers multiple attempted cyberattacks every day. Most of them cause little or no damage, because either the organisation's own system repels them or they are able to be resolved very quickly at a local level. At one level, you could say those are high-likelihood, low-impact attacks. Certainly on the telecoms network, the majority of outages that we find are caused by more mundane causes, so the effects of weather, particularly infrastructure problems, usually caused by accident but sometimes maliciously, as we saw in the recent case with attacks on 5G masts.

The really key point in relation to cyber is almost less about likelihood and more about impact. The reason cyber is particularly uppermost in everyone's minds and, certainly in our sector, the Government have chosen to legislate and place more prescriptive obligations is that if you get really sophisticated and serious cyberattacks—we have seen this in the last couple of week with the Hafnium attack via the Microsoft Exchange—they can affect multiple sectors and companies at once, and involve proper harm to the national and economic security of the countries affected.

Q148 **Lord Rees of Ludlow:** My question is primarily for Chris Train. I would like to ask about your assessment, based on your experience at National Grid and Cadent, of the general resilience of the gas and electricity networks. You are quoted as saying that we need not worry very much about solar storms. Would you like to amplify that? I would then like to ask about a couple of other things about the cascading of failures like we had a couple of years ago with the electricity grid. I would also like to ask about our dependence on interconnectors to mainland Europe, et cetera. I gather that we have had to draw on them in the past. If that is not available, does that not leave us in trouble? Would you like to comment first on solar storms, if we could be reassured on that, and on these other cascading issues?

Chris Train: For a bit of context, it was probably some time ago, when I was responsible for the control of the electricity transmission system,

that I made that comment on solar storms. What do I mean by that? You have to look at the specific risks and the consequences. A number of things had been put in place following the events of 1989 and 2003, where hardening of the assets had improved the situation. There was a lot of comparison around that time with the US electricity network, which is designed differently from the way the GB system is. It is like a matrix; there is a lot of strength within that matrix.

The other aspect of the matrix and the design conditions that were mentioned by Cathryn earlier—SQSS on the electricity network—means that a lot of the transmission system is part-loaded. There is a lower risk to the transformers on a part-loaded system. Alongside that, there have been great improvements in the forecasting of space weather. The Met Office, in particular, provides a space weather forecasting network. The early-warning aspects of a coronal mass ejection and its trajectory are much clearer now than they used to be.

Alongside those hardened measures and the forecasting, National Grid has a set of procedures in place that would be enacted to minimise any vulnerabilities. They would not eliminate all vulnerabilities, but they would minimise vulnerabilities to a coronal mass ejection. As you well know, it is on the national risk register. National Grid takes responsibility for operating the network and the system very seriously. In terms of a solar storm, we are probably better placed than we ever have been to manage that specific risk to the system and the network.

Lord Rees of Ludlow: As I understand it, in Canada they have very long cables. You build up a big electric potential and that is harder to deal with. We probably do not have that problem.

Chris Train: That is right. In North America, Canada and the US have long-run lines and are therefore more vulnerable to the induced current from the coronal mass ejection. That puts the transformers at risk, whereas, as I say, our matrix network gives us more resilience to such an impact.

Lord Rees of Ludlow: What about the separate issue of the risk of cascades, such as when a wind farm went down and then something else did, et cetera. Are you confident that we can minimise that sort of problem happening?

Chris Train: This comes down to the security standards that are operated. There is always a level to which you will protect the system. The current arrangements are that you protect the system to the largest loss on the system. You can end up with more than one fault at the same time on the network that is greater than the largest loss on the system. In 2007, the system lost Sizewell and Longannet almost coincidentally. That takes you out of the amount of reserve you keep in the system to be able to manage any disruption. The question is really around what level of resilience you want to protect against. You can always put more reserve in the system, but that comes at a cost.

As the system develops its increased diversity is a strength in terms of resilience. However, you need to look at the physics of the different characteristics and the way the system is managed and operated. It needs to be a dynamic risk assessment of the impact of the losses on the network.

Lord Rees of Ludlow: What about the issue of whether we need to import electricity from the rest of Europe?

Chris Train: Importing electricity through interconnectors has a combined effect. As we change our energy mix we need to ensure that we have electricity availability and electricity resilience. On the whole, that interconnection with Europe and Norway gives us enhanced resilience on the system, on the basis of open market and operations. The flows of electricity will follow the market signals and the need. In many ways it is akin to the cyberthreat: increased connectivity creates opportunity for increased risk. It needs to be made sure that that is managed appropriately. As we decarbonise the electricity system, interconnectors offer us enhanced resilience overall in our energy supplies.

Lord Rees of Ludlow: Except that they may not have the spare energy at a time we most need it.

Chris Train: That is correct as well. That has to form part of your overall risk assessment as to how the interconnectors' risk is applied to the security of supply and whether an interconnector coming from France has the same vulnerability as interconnectors coming from Belgium, Norway or Denmark. There is a level of diversity within the interconnection as well.

Lord Rees of Ludlow: Is there anything in your general remit of these grids that you think we should especially worry about and investigate more on this Committee?

Chris Train: In terms of the grid, the challenge is about how we develop the risk assessment as our distribution networks become what we would call active-controlled, so more distributed generation in the distribution networks. There is the development of the distribution system operator and its relationship with National Grid as the system operator. There is the increased development of the offshore grid for wind farms and ensuring we get the right level of risk assessment in the development of that offshore grid.

Q149 **Baroness McGregor-Smith:** This is a very general question, but hopefully we will get some interesting answers to it. How do you ensure that regulations are up to date and relevant, bearing in mind we have so many new technologies coming in? Thinking about the future of technologies and where they are going, I would be very interested in your perspectives on how we keep up to date.

Lindsey Fussell: It is a really interesting question. In the telecoms space, the speed and pace of network communications and the way they

have changed has been remarkable. That is never more so than in the past year, where we have all discovered that we want to use our home broadband for meeting like this, rather than for the activities we were using it for before.

I have a couple of points by way of starting the discussion. The first thing to say is that new technologies can really help with resilience. The move to full fibre is something we are really pushing for in relation to broadband. Full fibre is generally a lot more resilient than the old copper network we have at the moment. It is particularly more resilient to extremes of weather. We get quite a lot more capacity from 5G, particularly in urban areas, so you get less congestion on the network; it is that experience where you find you cannot download something on your mobile phone, not because the network is not working but because so many other people are trying to use it at the same time.

New technologies offer a lot to us in the form of enhanced resilience, but, having said that, they also bring challenges. Our reflection on the past year is that our networks have held up pretty well and the demand on them has been completely unprecedented. We have broken the daily rate for the most data used on our fixed and mobile networks multiple times during the course of the past year. I think Boxing Day may have taken the crown on the Openreach network for the highest load ever experienced. It also demonstrates that you cannot be complacent about these things.

We have put in a number of changes around that over the course of the past year. In particular, we have enhanced our ability to investigate the root causes of every incident reported to us, however minor. That is already giving us some benefit. For example, in the early days of the lockdown there was a brief period where there were some problems with mobile connectivity due to overload on certain points on the system. We have been able to identify the root causes of that and work with the operators to make sure that cannot happen again. There are other examples. I will not go into more detail. The point is that there are some good things and some challenges here, and you cannot be complacent.

On cybersecurity, it might be worth also saying that there is a code of practice that underpins the new legislation I have mentioned. I know that, from the Government's perspective, the idea of putting a lot of that in a code of practice is to be flexible and to be able to update that code of practice. Cyberattacks are clearly continuously evolving too.

Cathryn Scott: It is a very similar picture in energy. We are living through a time of immense change. One of the key challenges we face as a regulator is ensuring that our regulatory regime can keep up with the scale and pace of technical change. We know that the energy sector will need some dramatic changes in how we generate electricity. That is already happening, but there needs to be a lot more of it on how we heat our homes, how we power our vehicles and how electricity and gas networks are built and operated. We need to move from the system we have at the moment, which is still largely made up of large, flexible

generators, providing power on request and when required, to enabling us to be able to use smaller, intermittent generation. That comes with certain challenges.

We are very much building a toolkit to keep pace with the changes. For example, we have set our price controls for five years but built net-zero reopeners into our recent price controls, so that more investment can be unlocked partway through that five-year period to help to build necessary infrastructure as it is required. A reopener could be used if the Government decide they want to decarbonise gas and deploy hydrogen networks sooner rather than later, or if there is a decision to reinforce the electricity network to support EV charging infrastructure. We also have a similar reopener mechanism to fund cyber investment.

Another way we are trying to deal with this is prioritising several workstreams to support the energy transition. For example, our new draft forward work programme includes a programme to help support and unlock new sources of flexibility on the energy system. Flexibility is going to be particularly important in the future, as most low-carbon generation does not respond to changes in demand very easily. Wind and solar are reliant on the weather, while nuclear is generally quite slow to be able to respond to changing demands on the system. In future, we need to find new ways to match the generated output, through things like zero-carbon storage or ways of managing demand to match supply. Flexible technology will not just help us meet net zero but boost the resilience of our system as more intermittent generation comes online.

We are also working closely with the Government to support reforms to our energy system and to the legislative and regulatory framework designed to address the challenges of net zero. For example, on code reform, the energy codes are the rules that are industry-led; the energy industry complies with them. The process by which those rules are made is really clunky. We need modifications to these rules. We need changes to the way this works so that there is more strategic oversight.

Q150 **Lord Clement-Jones:** There are quite a number of technology opportunities and challenges there, from both Lindsey and Cathryn. I wanted to come on to the question of regulator skills in the face of these new technologies. You have set up the Digital Regulation Cooperation Forum, which is designed to try to link in between the regulators to meet these challenges. Do you have a particular focus in the DRCF on things such as risk assessment in the face of these new technologies?

Lindsey Fussell: As you say, the Digital Regulation Cooperation Forum is a relatively new development but a really important one. It is looking quite specifically at some of the challenges around digital competition, particularly around the new tech giants, the hyper-scalers and what kind of regulatory co-operation needs to happen to make sure those systems are operating in the best interests of consumers.

Although the DRCF is definitely an interesting development, probably for this purpose it might be worth talking a little more about some of the

other co-operation that we have going on. A number of you have seen the UKRN report published back in 2015. It talked about the need for much greater collaboration between the regulators, and specifically identified the interplay between energy and telecoms as being really critical here. Since then, we really have deepened that collaboration.

As an example of one of the projects that we are very closely engaged in, we have been working on a project for a couple of years now with the Energy Networks Association, which is specifically looking at what the needs of the energy sector will be as they digitise over the next 10, 15 or 20 years, and what connectivity they need to support that. For example, one thing we think they may well need is a dedicated radio spectrum—effectively their own private, dedicated network—to be able to promote that resilience. That kind of exercise is hugely useful to us because spectrum is a pretty scarce resource in the UK. By knowing it may be needed, we can factor it into the long-term spectrum management plan, consult other users of spectrum and make sure we are really sighted and promoting the right resilience for our energy networks. That kind of exercise is a really welcome development in our collaboration.

We have also come an awfully long way in collaboration on cyber. That has moved on a lot since 2015 in everyone's understanding in the UK.

Lord Clement-Jones: Cathryn, I was going to ask a supplementary, as well as the question I put to Lindsey, as to whether the idea of a centre of excellence in this area is an important one. It is mentioned in passing in the DRCF workplan.

Cathryn Scott: By centre of excellence, do you mean some kind of central co-ordination of resilience?

Lord Clement-Jones: Yes, exactly, and dealing with, say, risk across these new technologies.

Cathryn Scott: In terms of cyber resilience, the existence of the National Cyber Security Centre and the co-ordinating role that it plays across all the different areas is extremely valuable. On other types of risk, there may very well be added value in some kind of central resource, but how far are there similar problems? There are clearly some similar problems.

Q151 **Lord Browne of Ladyton:** I am going to invite Chris Train to deal with this issue from the perspective of his experience. Within the energy industry—at least the lobbying I have had as a parliamentarian suggests this, and it is true—there is a great pressure from consumers, Members of Parliament and the Government to keep down costs for consumers. This cannot of course be at the expense of security or proper infrastructure spending. We need to keep resilience up. How well does your experience suggest that the regulator of the energy industry balances the competing requirements of keeping prices to the consumer down and infrastructure, security and other spending up?

Chris Train: That is a very complex question. In a way, the answer is very similar to the first question, which was, if you recall, around the

mechanisms to ensure the resilience. Therefore, it is a discussion and a dialogue as you go through the relative price controls. That is always a very challenging experience from a company's level. It also encourages new ways of thinking and of doing things. In that respect, it is quite helpful.

The company will put forward its view around investments in assets and in operations. It will put forward its case and its business plan, which is then assessed by the regulatory team. There is usually some form of consulting support to add the expertise into the regulator for it to be able to assess those business plans. A judgment is then made through the draft determinations. That then enters into a formality of, "You have not proved your case on this, you have proved your case on that." Ultimately, the assurance for the regulator is whether the price control gets accepted. As an organisation, you are responsible for the resilience and security in your network and its compliance with the standards.

From a personal basis, it is quite a challenging process. In essence, that is the mechanism. You balance out that pressure around the resilience and the operations. That comes down to a judgment element at the end of the day. Your network will comply with the standards and obligations, whether that is SQSS in electricity or the one in 20 obligation for delivery on the gas networks. There is always pressure on short-term costs and it is part of the regulatory role to ensure that they are looking at not just today but into the future. That is particularly the case as we are going through what is or will be a very dramatic energy transition.

There was one thing I wanted to mention on one of the previous questions, but it sits in here as well. There is a risk of looking at individual asset resilience rather than systemic resilience. One of the strengths around our energy system is actually treating it as an energy system. As we go through decarbonising that energy system, that level of interactivity and the looking at it as a system becomes more and more important.

Lord Browne of Ladyton: This is a different question but it is related, as I hope will become apparent. Lindsey, in answer to the first question you mentioned increased demands about security that had been placed on the industry by the Telecommunications (Security) Bill. Indeed, you gave evidence to the Public Bill Committee on 19 January. When asked about the increased demands that were being placed on Ofcom by that Bill, you were very candid about the challenges you were facing in building up a team to face this. I am particularly interested in any barriers or issues that may hamper your ability to be able to do that. Specifically, you mentioned that, in recruiting a team, you were drawing people from the operators and you honestly accepted that highlighted a problem. Is there a skills gap? Is there a scarcity of expertise? Are too many people competing for the same resource in this space of security in your industry?

Lindsey Fussell: There is no doubt that cyber skills and cybersecurity skills are in great demand, not just in the telecoms industry but across

the UK economy as a whole. That is inescapably the case. In relation to Ofcom's position, we already have a network security team in place because we have some existing responsibilities in this area, so that certainly helps. To take on our new telecoms security responsibilities we are expecting to grow that team by a further 50 people across the organisation, although not all of those will be cybersecurity skills; some will be on the legal and enforcement side.

On recruitment, we find that we have to pursue a number of different options. We certainly find that we are able to attract people in from the operators with cybersecurity skills. That is clearly hugely helpful to us, because they also have really good knowledge of the way networks operate in practice. We also have to think about, for example, building a pipeline, so thinking about the graduate programmes that the National Cyber Security Centre endorses and how we draw people from that at an earlier stage in their careers to build their expertise. Finally, secondments can also be extremely valuable as part of this. It is not straightforward, but it is something we are already on the path to. Although we absolutely do not underestimate the difficulty of it, we are confident that we will secure the skills we need.

Picking up on Lord Clement-Jones's question, this is also relevant. The DRCF has a specific strand in its workplan about sharing skills and experience between the regulators, joint recruitment and so on. That is also true of the cybersecurity forums that the regulators take part in that are run by NCSC. There is also something here in us sharing resource and expertise, when it is appropriate to do that, to maximise the skills and capabilities we all have available to us.

Lord Browne of Ladyton: Are there any other resources that are challenged by the responsibilities you are being asked to take on? Do you have sufficient money?

Lindsey Fussell: Yes. We are in discussion with the Government about the additional funding that will be allocated to Ofcom for telecoms security and the likely new upcoming responsibilities on online harms. We expect that we will be sufficiently resourced to take on those new responsibilities. That builds on the expertise we already hold in the organisation.

The Chair: Could I ask you to translate DRCF and NCSC?

Lindsey Fussell: I am so sorry; I am afraid we are hidebound by acronyms in regulator land. DRCF is the Digital Regulation Cooperation Forum. NCSC is the National Cyber Security Centre.

Cathryn Scott: Our experience of the issues of cyber skills is very similar to Lindsey's.

Q152 **Baroness Symons of Vernham Dean:** I wanted to come back to this question of the costs. In the paper the Government published yesterday on the integrated review of security and defence, et cetera, they say, in

their major annexe, that £305 million of continued investment for 2021-22 for the cross-government national cybersecurity programme should cover transformational cybersecurity projects. There is a further £18 million for 2021-22 for international cyber. Were you consulted on those costs? Do you think those costs are sufficient for the sorts of transformational developments you have been discussing with us?

Cathryn Scott: From Ofgem's point of view, I am not aware that we were consulted on those costs. The costs of cybersecurity and cyber resilience are not simply that kind of funding. The network companies and operators of central services effectively fund their cyber capability and those costs are passed on to consumers. For network companies, it will be through the price control, which is why we test their cyber proposal as well as their other resilience proposals as part of the process of the price control. That amount of money is a drop in the ocean compared with how much will be put towards cyber resilience.

Baroness Symons of Vernham Dean: This is talking about transformational cybersecurity projects, not just maintenance at the moment. It seemed to me an extraordinarily low sum of money if you are really going to talk about the transformational costs. There is a further £18 million for international cyber and digital and data capacity-building programmes. Again, this seems a very low figure for the sort of transformational vision that many have for cybersecurity in the next few years.

Lindsey Fussell: To add to Cathryn's point, it is difficult for us as regulators to comment on that. It is the Government who take the policy lead on cybersecurity. The amount of public funding that they think needs to go to those kinds of activities is not something we would expect to be involved in or determine. Exactly as Cathryn said, in relation to telecoms security, the legislation I have been talking about explicitly does this: it places the obligations on the regulators to invest very significantly in the security of their networks, but the cost obligations are on them to do so, rather than on the Government to fund that.

Q153 **Lord Triesman:** I think Lindsey Fussell answered a lot of this in relation to Lord Clement-Jones's question, but there appears to me to be a bit of a difference between some of the things we are being told. Early on, in response to a question, Cathryn Scott said that each risk is very important in its own way. We have also heard that the degree of co-operation between regulators is very much higher. I can remember when the Better Regulation Task Force in the Cabinet Office asked similar questions, albeit some time ago. It was always thought that a lot of co-operation between the regulators was a disproportionate demand on them. Do they co-ordinate or not? I am quite interested as to whether Mr Train has a view. He smiled knowingly at that moment.

Lindsey Fussell: Speaking honestly and personally, I do not think the co-operation between the regulators is in any way a disproportionate burden. I know that UKRN will soon be publishing its multiyear workplan. It is going to look at a range of things that are really pertinent to a lot of

us, such as vulnerable consumers, particularly financial vulnerability. The type of consumers we are all dealing with in relation to debt, as we come out of this pandemic and the furlough scheme and others come to an end, will typically owe money to people across all our sectors. How that is dealt with is relevant to all of us. Some of these issues we have been talking about today, about resilience and cybersecurity, are also clearly very relevant to all of us. I do not feel it to be a disproportionate burden at all.

As I was saying, there has always been a really close interconnection between the energy and the telecoms sectors. Fundamentally, telecoms depends on power and energy is ever-increasingly dependent on communication. The type of project that I was discussing that we have been doing with the Energy Networks Association is critical to both regulators and both sets of industries to make a success.

Cathryn Scott: I completely agree. A lot of co-ordination goes on. In one of my areas, which is enforcement, I have recently been speaking to all of my colleagues; we chat about the challenges we are facing, how we address them and common themes. The UKRN is a really good way of making sure we are working closely together. As we go into the future, as the system digitises and changes, it will become increasingly important to adopt a whole-system approach and to have more cross-regulatory engagement. That is something we are considering really carefully and working on.

Lindsey has already given the example that, as we move from copper cables in telecoms to fibre optics, they are going to be more reliant on power. Any major energy incident would have a greater impact on communications. Conversely, as the energy system becomes increasingly digitised, parts of the energy sector are going to become more reliant on the internet to communicate. We are looking at those kinds of challenges together. As things emerge, I am confident that we will be able to work together effectively on these kinds of issues.

Chris Train: My smile was at the recollection of the Better Regulation Task Force, so apologies for that. It is very important that the regulators talk and co-ordinate activities, particularly as the cyber risk has increased. The open-source information networks particularly mean that Ofcom and Ofgem have a role in ensuring good communication is occurring between the two. The critical dialogue, which has always been very good in the energy sector, is the Government—so BEIS as the department responsible—Ofgem and the industry meeting regularly together to understand the risk and resilience, and to ensure that the appropriate investments and plans are put in place. This is done formally through the structure of the Energy Emergencies Executive, but also informally as we go through the change as well. I would encourage that dialogue going along.

Q154 **Lord Browne of Ladyton:** Since we have slightly overrun our time, it is time for short questions and short answers. The short question here is about how providers are required to communicate with the regulators and

their customers in the event of a reportable incident or emergency.

Lindsey Fussell: Under our existing Communications Act, operators are required to tell us of any incidents that have an impact on their operational performance. We would regard that as certainly including, for example, all cybersecurity incidents. Under the revised legislation that is coming up, the Telecommunications (Security) Bill, they will be required to tell us of incidents that not only have caused an immediate operational impact but might cause an impact in the future. That is quite important, because, when it comes to cybersecurity, quite often what you find is that there is something that may not appear to be a big problem initially but actually creates issues for the network further down the line. Those are their responsibilities to us.

There is no specific requirement on consumers. We have backstop powers. We can direct them to tell consumers of incidents and, again under the new legislation, advise consumers of things they might need to do, such as changing passwords. We have not tended to need to use those backstop powers. Providers pretty much tell consumers at the same time as they inform us. It is almost always in their interest to do so. If they do not and there is an outage, for example, they will find themselves besieged by consumers who are trying to get in touch with them to tell them there is a problem. In our experience, they are pretty good at informing consumers direct, but we have those backstop powers there if we need them.

Cathryn Scott: It is very similar on the energy side. There are very clear reporting thresholds and processes in place for the companies to report certain serious energy incidents. They report to us. BEIS is leading on emergency preparedness and would, in the event of a major incident, activate an emergency response arrangement. We then support that as part of the team and provide guidance on things that we know about, such as market operation, whether the industry rules need to be changed and whether the regulatory arrangements need to be switched off.

On communications with customers, the duty officer will consider when considering how to respond to an incident the media communications and whether and how the market has been informed, among other things. There are also licence requirements, such as an obligation to contact customers on a priority services register. Those are vulnerable consumers who might be more reliant than everyone else on electricity and gas. We enforce against failing to do that, so that is something we take into account as well.

Lord Browne of Ladyton: I will follow up with a short supplementary. On network information systems regulations, Ofgem's guidance mandates reporting of these incidents, when they have reached the threshold for reporting, within about 72 hours. It also encourages and notes that, if there is an NIS incident and it involves cyber, you should not wait until it gets to the reporting threshold before you go to the National Cyber Security Centre. I have not seen this for myself, but I am advised that Ofcom's guidance sets out similar requirements. What is your

experience? How promptly are providers reporting such incidents to regulators or to the National Cyber Security Centre?

Cathryn Scott: There are reporting thresholds that are set out through NIS, which are very similar to the reporting thresholds we have generally through the licensing arrangements for the more general issues. There have not been a huge number of issues that I am aware of that have been reported, but we certainly make sure that the operators are aware of the requirements. There is an issue about the fact that there are powers for us to be able to explore what are called near-misses, where something might not happen but where there might be lessons to learn. We can ask for that information as well. We and BEIS are considering whether in future guidance we want to put requirements on OESs to notify us of near-misses, where there was not actually an impact but there could have been.

Lord Browne of Ladyton: As a regulator, how do you assess compliance with the guidance, as to whether all of these incidents are being reported?

Lindsey Fussell: To clarify on the NIS guidance, in our case we are the competent authority for certain digital infrastructure functions on the internet, particularly some domain name hosting services. Those are not services that have direct customers in the same way that our network providers do. Our network providers are actually caught by our Communications Act responsibilities that I was discussing before.

To go back to your question on NIS, the approach we have taken there is, having identified the companies that fall within the scope, in 2019 we carried out a questionnaire to assess how well they managed risk and how ready they were to mitigate and respond. We used that as the basis of the assessment. The changes to the regulations, which literally just came into force in December 2020, have strengthened our ability to collect more information and enforce against the regulations. We are now thinking about how we amend the guidance to take account of that.

Generally, we would, as part of NIS and under the Communications Act, encourage all our operators to report major incidents as soon as possible. In relation to our operators, we have reported to us normally between around 400 to 700 incidents a year, to give you a sense of scale.

The Chair: Will you forgive me if I bring this particular panel to an end? I am conscious that we have another panel to start and we need to move on. To all our witnesses on the first panel, thank you very much indeed for your evidence, which has been very interesting and most useful for our report.