HOUSE OF COMMONS

Treasury Committee

Oral evidence: IT Failures in the Financial Services Sector, HC 1766

Wednesday 24 July 2019

Ordered by the House of Commons to be published on 24 July 2019.

Watch the meeting

Members present: Nicky Morgan (Chair); Rushanara Ali; Mr Steve Baker; Mr Simon Clarke; John Mann; Alison McGovern; Wes Streeting; Alison Thewliss.

Questions 210-309

Witnesses

I: Alison Barker, Director of Specialist Supervision, FCA, Lyndon Nelson, Deputy CEO and Executive Director, Regulatory Operations and Supervisory Risks Specialists, PRA, and David Bailey, Executive Director Financial Market Infrastructure, Bank of England.

Written evidence from witnesses:

– FCA, PRA and Bank of England

Examination of witnesses

Witnesses: Alison Barker, Lyndon Nelson and David Bailey.

Q210 **Chair:** Good morning, and thank you very much indeed for being here for this latest oral evidence session on IT failures and operational resilience. I am going to ask the panel to introduce themselves, and then we will get on with some questions. It is very warm in here, so you can remove your jackets. That's probably about it, actually—*[Laughter.]* I was going to say that you can take your ties off, but let's not get carried away, unless it gets really, really unbearable in here. In which case, please do so, and please carry on drinking lots of water. Mr Bailey, we will start with you.

David Bailey: I am David Bailey. I am the executive director of financial market infrastructure at the Bank of England.

Alison Barker: I am Alison Barker. I am the director of specialist supervision at the FCA. My remit includes cyber and technology.

Lyndon Nelson: Good morning. I am Lyndon Nelson. I am the deputy chief executive of the PRA.

Q211 **Chair:** Lovely. Thank you very much. I want to start with an overview question. I think it would be fair to say that operational resilience has risen up the agenda and is very important to all your organisations. Perhaps, Mr Bailey, we will start with you. How do IT failures within the financial services sector affect the Bank of England's objectives?

David Bailey: The specific institutions that I am responsible for supervising, as compared with Lyndon and Alison, are financial market infrastructure—the payment systems, the security settlement systems, and the central counterparties, which provide systemically important services to the wider financial sector and consumers. Therefore, we take operational resilience very seriously. Any outages can very quickly have a broad impact. The impact will depend on the type of financial market infrastructure. Payment systems, as we saw with outages at, for example, Visa, which the Committee has looked at, can very quickly impact individual consumers. Some of the other types of financial and market infrastructure are more wholesale market orientated. Therefore, the implication of any outages there are more around the liquidity that is available to the firms that use them. However, by definition they are all systemically important, so any issues with their operational resilience can very quickly spill into a financial stability issue.

Q212 **Chair:** Ms Barker, perhaps you can put operational resilience and IT failures into the context of the FCA's objectives.

Alison Barker: Operational resilience has been one of our core priorities for the past three years; it is something we are very focused on. From the FCA perspective, we want to ensure that markets work well, particularly for consumers, so our focus is particularly on the types of responses to operational outages and the continuity of services for consumers, and how firms are able to manage that.

We have three core areas we are focused on in that regard, including the policy agenda, where we have worked jointly as authorities to think about what the policy framework should be—no doubt we will talk a little bit more about that. For us, there is a key challenge in communicating to 58,000 firms what it is we would want them to take notice of in relation to operational resilience and their consumers, so we have a very focused agenda around that.

We also have a very focused supervisory agenda looking at standards, and we are also particularly focused on the incident management—so, when incidents do occur, how are consumers treated and communicated to in that environment. Those are the core areas of focus for us.

Q213 **Chair:** Mr Nelson, in the same context, how do IT failures and operational non-resilience impact on the PRA's objectives?

Lyndon Nelson: There are really three layers going up in the scale of impact, given that we supervise some very small banks and insurance companies and also some very large banks and insurance companies. At the lowest end, it is essentially the ability of management to run their bank or their insurance company if the IT system is gone. If the IT system continues to cause a problem, then we may be getting into the safety and soundness of firms, which is really a prime interest of the PRA. Then, fundamentally, it could also then cause either a financial stability or systemic issue if it then has knock-on consequences, as it would for one of the major institutions, for example.

Q214 **Chair:** Obviously, you have the joint discussion paper. You all have elements of the paper that you will be able to answer for; I am not sure who wants to go first on this one. I guess it would be helpful to know what responses you have had to the discussion paper, and what the next steps are in terms of a consultation paper.

Lyndon Nelson: It is probably one of the most popular discussion papers we have produced. I think that is partly because it has got a wider audience, because we have joined it with the FCA and our colleagues.

Q215 **Chair:** Sure. Do you think it is also because you have got ahead of a curve, in a sense? It is not trying—well, there are problems that have occurred, but you are also trying to look to the future.

Lyndon Nelson: Yes, it is definitely different, in terms of it being a more outcome-based and principles-based document than regulators have published in a good while. Certainly from my context at the G7 group, which I co-chair, I'd say we are first out of the block with that sort of thing. It has received a lot of positive comment, as I think some of the evidence you have already taken suggests. The main constructive comment we have had back is that the firms are trying to work out how operational resilience fits in with some of the other requirements that the regulators already have on operational continuity and resolution, or in terms of operational risk and the capital they might hold against that.

We intend to come back in about October with a consultation paper. I cannot be too precise on the date, because of course we have four governance processes to go through. We prize the collaboration very highly, and I think the industry also likes that, but it just means I have four governance processes. Around October, we should be coming back with some proposals.

Q216 **Chair:** In the written evidence, you—I say "you", but I think it was a collective, joint thing—explained that "adequately guarding against disruption does not require a zero-disruption regime". Can you unpick that? Perhaps you can all say this regarding your own fields. If not zero disruption, what is the tolerance, who sets it and at what point are you not tolerant of the disruption that has happened? I do not know who wants to go first.

Lyndon Nelson: Shall I go first? It might be helpful, just in the policy space.

What we can contemplate is that there will be effectively a tiering of the tolerance, as you have put it. There will be effectively four authorities potentially setting tolerance. The Financial Policy Committee will be interested in financial stability issues, such as for how long the payment system will have to be out before this gives rise to an issue. Then there will be David and I in the middle, about the safety and soundness of the institutions, and as David has already highlighted he gets pretty close to those financial stability events almost automatically. Lower down, I think there will be Alison, with the interest in both the consumer and the markets. The FPC is currently carrying out a stress test, which will help it calibrate where its tolerance will be, and then we will work within that.

There are existing standards. David is probably the best one to talk to, because the only ones out of the gate at the moment internationally are the payment systems, where they do contemplate both a recovery time and some opt-outs. Perhaps David could talk about that. We will then set a tolerance—Alison will be the same, I think—that is suitable to our objectives, when we think the safety and standards will be affected and when the consumer and market objectives are impacted for the FCA.

Q217 **Chair:** Alison, perhaps you can pick that up. So tolerance is set, so people will know at what point it has tipped over into something where there has to be—

Lyndon Nelson: Yes. What we also foresee in the policy is that we obviously expect the firms to set the tolerance. We would comment on that.

Q218 **Chair:** Okay. So they set it and then you comment on it.

Lyndon Nelson: Absolutely.

Q219 **Chair:** Ms Barker, anything to add on the FCA perspective about zero disruption?

Alison Barker: Yes, let me pick up the last point Lyndon made. With 58,000 firms and such a variety of firms, in the first instance we expect them to understand what business services they have and what it is that consumers should expect from them so that we can understand what is appropriate for each type of business and each type of consumer group they serve within those businesses.

A one-size-fits-all approach may be challenging within the context of the vast array of types of firms we have, but we are focused on firms being clear in the first instance that they understand what their business services are and understand their consumers—in particular vulnerable consumers and how they should be treated in that context and what they might do. When you talk about the sort of zero tolerance, zero failure—

Chair: Zero disruption.

Alison Barker: Zero disruption, yes. I think the key thing all of us as regulators have been focused on is that, although we want firms to focus on prevention of disruption and plan properly, particularly around changes of management, particularly in the cyber environment, where things can

be unpredictable, we also have strong messages around, "Be prepared. Make sure you understand how you will respond and recover from an incident. Don't focus on prevention at the expense of what to do when something happens." That is because firms that are not well prepared cause more disruption to consumers.

Q220 **Chair:** Mr Bailey, perhaps you can pick that up and the existing standards that Lyndon mentioned.

David Bailey: Yes, I will start with that. As Lyndon mentioned, we already have some international standards in the area of financial market infrastructure which reflect their systemic importance. They are that: all FMIs should have plans in place to be able to recover from an outage within two hours; but certainly to ensure that all payments are settled by the end of the intended value date. So by the end of the day, all payments should have settled. The only exception to that is in the case of a cyber-attack which compromises the data integrity sitting within a financial market infrastructure, because quite frankly it is not worth coming back up if the data is corrupted. You may in fact promulgate the problem rather than solve the problem.

Those standards have been in place since 2012. We contributed to their development, and we hold the FMIs that we supervise to those standards in terms of what they need to demonstrate to us. But they act as a baseline. One of the points that Lyndon made was that it is important that individual firms and FMIs set their own tolerances, and that is where we are pushing them. For some, it may be appropriate to have an even shorter recovery time, and that is what we will expect them all to develop once we move forward into our policy making phase.

Q221 **Chair:** Is there hope that, if the consultation is picked up, customers will experience fewer disruptions or fewer significant disruptions? You talked about outcomes; what is the ultimate goal?

Lyndon Nelson: You would hope that would be the outcome of the policy. One may reflect that in some of the instances we have seen, there really was not an adequate plan B.

Q222 **Chair:** Right—so it is about making sure that everyone has a good plan B.

Lyndon Nelson: Exactly. As Alison said, if the hypothetical service—somebody getting their mortgage granted or their deposit paid—is primarily delivered through a computer system that is now out, what is the plan B and does it deliver within the tolerance that we set? One would hope that when the policy is fully through, consumers and constituents will see something very different. They will get their service—it may be slightly clunky or slightly late, but it certainly will not be at the level of disruption that we have had so far.

David Bailey: They will also get better communication throughout the issue, which is really important.

Lyndon Nelson: I was going to come to that, yes.

David Bailey: It has been a feature of some of the incidents that we have seen historically that firms have looked to solve the IT problem without managing the broader incident.

Chair: We will come on to consumers and everything else—that is very important.

Q223 **Wes Streeting:** Good morning. We heard evidence last week from those who are regulated and supervised about their experiences of interaction with each of your institutions. I want to focus on the skills and expertise to do this job properly. To what extent are specialists used in any supervisory engagement on operational risk and resilience issues?

Lyndon Nelson: For the PRA, I would say that at the moment it is almost exclusively a specialist activity. In other areas of risk specialism, it tends to be a bit more of a partnership with supervision. To give you an idea of the numbers, we have about 560 supervisors and about 40 specialists in this particular field. We are doing training exercises for supervision, to get them slightly further up the curve, but at the moment it is almost predominantly delivered through specialist activity.

Q224 **Wes Streeting:** You gave us some numbers. How many of those are technology specialists?

Lyndon Nelson: About half of those 40 are technology specialists. I tend to find in this area that it is as much about people and processes as it is about silicon, so that is probably about the right mix, we think.

Alison Barker: From the FCA point of view, we think about this first and foremost in terms of the overall approach to supervision, because it is a core part of our objectives and our supervision work. Our starting point is thinking in terms of the governance and oversight of firms and what they are doing. We have 900 supervisors, so we would expect some element of understanding of what is happening to be covered by supervisors generally.

We then have 400 staff within authorisations. At the gateway, we would specifically look at technology resilience as a matter of the authorisations. An example of that is when we have assessed the payment services firms as they have come in, looking at technology, and the AISPs, which are part of the Open Banking infrastructure.

We then have 40 specialist staff, who have a mix of technology and cyber skills and backgrounds. They have 16 different types of qualifications between them, in subjects from IT audit to cyber-security or intelligence. The specialists support the supervisors and supervisory staff in their technology assessments; they also carry out specific technology assessments.

We work with the Bank on certain types of assessments. We have not mentioned CBEST yet, which is the specifically designed pen testing approach that, in simple terms, looks at questions like "How can we hack a bank?" We do that with the Bank; we have people on it, but we also use accredited external parties to run some of that, so we have access to external specialists who we utilise, as well as our own.

Where we have needed to, we have also pulled together specialist teams to focus on particular types of big technology change. We have pulled together a department of 45 staff for two years who are focused specifically on the ring-fencing and on change management of the five banks that went through that process.

Where we need to, we have deployed dedicated resources. We have a specialist team of technology and cyber skills, and we have a general approach to supervision, of which this is a core part.

David Bailey: From a financial market infrastructure perspective, my numbers look a lot smaller than Lyndon's and Alison's, but that is because we supervise a very small number of FMIs: 11 firms, although they are all very systemically important. When you look at what those firms do, especially in the payment systems space, the risk they run is more about operational than financial resilience. They do not necessarily take financial risks themselves—some FMIs do, but not all.

We have about 40 frontline supervisory staff. In addition, we have a specialist team, of which about four are specialists around operational resilience. But we draw more broadly on Lyndon's team in the PRA. We use that resource very fungibly, both to do individual firm assessments and also thematic work across banks, supervised by the PRA, and infrastructure supervised by the Bank.

As Alison also mentioned, we make quite extensive use of external resources, so that we can commission expert resources to come into a firm and perform assessments, which adds to the expertise we can draw on.

Q225 **Wes Streeting:** You all describe the situation as it is. We have heard that regulators need to improve their expertise in relation to operational resilience. Lyndon, you are already nodding. That is something that you would agree with.

Lyndon Nelson: Yes. If I look at other types of risk that we deal with, that equation of how much is done by specialists and how much by the general supervision staff, those percentages would be remarkably different from where we currently are.

Because it is a relatively new area, we are having to do training for supervision. That is obviously all part of our personnel strategy about different skills for the workforce. Yes, we would acknowledge that we have to get the supervisors further up the curve. But I think the specialists are doing a good job as it is.

Q226 **Wes Streeting:** If I read body language correctly, that is a shared view. There is a recognised need to improve things. Could I ask each of you to elaborate a bit on what you are doing to improve the skills and experience, such as training and keeping skills up to date?

Maybe you could also give us an insight into some of the challenges that you face in trying to do that, whether that is recruiting and retaining the right people. Are industry secondments a viable option? Maybe you could

just talk us through how you see this. If you have accepted the need to improve, I assume you are all doing something about it, so tell us.

Lyndon Nelson: Shall I describe the training? The specialists we hire, and that David uses as well, are typically drawn from industry. We will obviously increase the number. In some instances, I would say that the industry itself is not particularly well developed in this area, so some of the skill sets are relatively rare. We may actually be faced with building our own.

One of the advantages the regulator has is that, because it sees the whole market, we can build those people up relatively quickly compared with the industry on its own. We are building up a supervisory framework: how supervisors will assess operational resilience and where they will prioritise their review and resources. Attached to that will be training.

I think the main constraint, to be honest, is probably a budgetary one. We have a number of other priorities. If members have read the Governor's Mansion House speech, they will know there is a lot happening.

I am happy with the resource settlement that we have got. I am partly responsible for the budget, so officially I suppose I have to be. We could go quicker if we had more, but I think it is the right balance. At the moment, we are going as fast as we can. I think the training course is probably going to deliver a much more effective outcome. It will certainly make us use our specialists in a more effective way.

Alison Barker: Much like Lyndon, we are sharing a lot of the training approach to the building and the supervisory frameworks between our institutions. A firm needs to have that shared view between the authorities, the PRA and the FCA. It needs to be seamless from that point of view and a lot of that work is done together.

From a general supervision point of view, building out those sorts of toolkits. On training for supervisors, I agree exactly with Lyndon. For our specialist staff, as I mentioned, there is a range of qualifications that our staff have had and those are often subject to CPD requirements, so there is continual learning.

The industry, particularly on the cyber side, is evolving very quickly. That is where the challenges for resourcing can come, in that that is quite a tight market and everybody is looking for people who can do cyber work.

Like Lyndon, I agree that one of the benefits of coming to a regulator is that we see such a broad spectrum. For people who are looking to build their careers in this space, we can often be quite an attractive employer, because we can see a wider range of things. We do find that and do work on that. We are continually working on our specialist skills and encouraging everybody to build those.

Q227 **Wes Streeting:** Just on that competitive market, before I bring David in, everyone is fishing in the same pool for a limited number of specialists. That is a very limited talent pool. Does that make salaries a

challenge? Are you able to pay people enough to get the right people in, or is that a challenge for you as a regulator?

Alison Barker: It can be, but we focus on what benefits you get from working at a regulator. People often come to work at a regulator because there is a sense of purpose. We are very committed to working to make the markets work well and for consumers. People who want that type of experience will want to come to regulators, so we have some things that firms don't have. We are keen to attract the sort of people who actually want to come and work for us, not just for the money. We try to emphasise those sorts of benefits. Money can be an issue, but we try to focus on the other benefits of working for us.

David Bailey: Just to pick up on the question you were asking about supervisory expertise, the real positive is that we are doing it all together. That means that the supervisors are all developing a common way to think about these issues and then talk about them. That is important, because you can look at operational resilience from an individual firm perspective, but we also need to think about the system as a whole. If one of the banks that Lyndon regulates has an outage, that can have an impact on the infrastructure that I regulate, and vice versa. We need to think about it on a system-wide basis, and developing a common framework to do so is really important. We are moving that forward.

I echo Alison's point about recruitment and retention. People come to work at the Bank for a wide range of reasons—not just money. That is part of the overall package. Therefore, it is possible to get the right people in. It is also a struggle to retain them, but at the moment we are able to attract what we need.

Q228 **Alison Thewliss:** The financial services sector is undergoing a huge amount of change, with new technologies coming in and other things going on. A significant proportion of that change is due to regulatory requirements changing. Is that volume of change creating operational risks for firms? How should firms deal with that?

Lyndon Nelson: We publish statistics that say that change is possibly one of the biggest drivers of failure. We can't deny that quite a lot of that change is regulatory, so the answer to your question is yes. A couple of things need unpicking there: one good and one murky. Firms often voluntarily partake of a lot more change, because they are under the hood, in a car sense, and while they are there they may as well make more changes. Some of the numbers relating to how much is driven by regulatory change can be exaggerated.

The amount of regulatory policy change that has been going on in the last 10 years, as we have been recovering from the crisis, is undeniable. In my 30 years, it is unprecedented. That seems to be tailing off a bit. I would argue, though, that if you now look at the business plans of the firms that I look at, the amount of change will continue, because they will be driven by commercial imperative if nothing else. Change is with us. It is a question of how one manages that change. Clearly, the Treasury has been receiving comments about the change that we cause through regulatory change, and you yourself received evidence from UK Finance about that. I

think that there may well be some responses. We are all working together on how we might "air traffic control"—I think that is the phrase—some of that. We have some responses, but it is not going to lead to a no-change environment, because I think they will simply use the weekends they would have used for regulation to improve their business model and make themselves more competitive.

Alison Barker: I would add some examples of where we work together to try, as Lyndon said, to "air traffic control" it, or be joined up. It is very important, as regulators, that we are joined up. The example you will have seen is where we worked together as financial regulators on the DP on operational resilience. There was a very joined-up approach.

The other thing to say is that there is a lot of change, whether it is regulatory, technology and digitisation. There is a lot of innovation in the financial services space, and as regulators we welcome that because it brings new services to consumers and takes forward the way in which markets work and think. Chris Woolard, our executive director on strategy and competition, was invited to Congress last week to talk to the financial services taskforce about the work we have done on innovation, open banking, sandbox and other innovative approaches. The US is very keen to understand the models that we have here.

That level of change will continue. We as regulators need to be focused on how firms manage change. As Lyndon said, the statistics show that that is often the greatest outage. While there is something about regulatory change and co-ordination, and making sure that we understand how change is landing on firms and that we do not contribute to the risk that they are going through, at the same time we want to make sure that firms are well prepared. It goes back to the point that they have to have thought about their plans to implement change: how to deal with what goes wrong; as Lyndon said, what the plan B is; how we manage that; and how we manage the communications. Again, that comes back to all the things we were talking about through the approach to operational resilience.

David Bailey: I would add that, yes, change can bring some risk, but in many cases, not making change can also bring risk as systems move towards obsolescence. Therefore, it is important that firms and infrastructure are thinking very carefully about what changes they need to make, and that they have clear internal governance and oversight of the changes that they are making with the right level of assurance. It is that kind of, "Have you got the right governance? Have you got the right level of assurance? Have you got clear structured plans?" Those are the things that the supervisors are in asking the firms.

Q229 **Alison Thewliss:** Alison and Lyndon, you mentioned the air traffic control notion. What does that look like for you? Is it a person, a role or another layer on top of other things? How would that actually work in practice? How does it become meaningful for firms?

Alison Barker: It is a matter of just getting going—getting off the ground. The Treasury published the call for input only last Friday. The chief executives of our organisations, the CMA and the Payment Systems

Regulator are all very committed. There has been a discussion with the Chancellor. They will take forward what ideas come through the call for input. There is an idea that there will be some consultation or wider discussion later in the year.

Lyndon Nelson: I have seen it in the Basel Committee, which is the global standard setter. Obviously, there are 23 jurisdictions there, so it is a bit more complicated than ours. When we are trying to agree implementation dates, we essentially have a group that looks at what the pressures are—the EU parliamentary timetable versus the congressional one and all of those. We try to get some sort of harmony and make sure that we have things, as it would be with air traffic control, landing with gaps, rather than three planes at once. It can be done, but it will obviously involve some difficult choices for that group.

Q230 **Alison Thewliss:** UK Finance has argued that the operational risks of change caused by regulation are exacerbated by an absence of co-ordination between public authorities over substance, timing and prioritisation, which speaks to some of what you said there. Do you assess the cumulative burden of regulatory change on firms?

Lyndon Nelson: That is always difficult to assess, I would say. Certainly, global firms that have multiple jurisdictions have been hit by a plethora of standards. My G7 group monitors that and there is a lot going on. They are making a valid case. The French presidency of the G7 has essentially pushed to try to harmonise it a bit more in this space. The news is relatively good there. Basel is coming up with a G20 standard. David has already spoken about his. We may get some answers there.

I do not really accept it in terms of domestic, because domestically, the discussion paper is the latest in a very collaborative effort. Actually, I would include the industry within that. We have been working very closely with them, regulator to regulated. I would not accept it domestically, but for the global firms, there is no question but they have been hit by a variety of different standards. Until we have a G20 standard, that will continue.

Q231 **Alison Thewliss:** On the work with international regulators and cross-border standard setting, can you tell us a bit more about how you work within the domain of operational resilience? Has the prospect of Brexit had any effect on our part within that international working with other EU nations and other international regulators?

Lyndon Nelson: It has had zero effect, I would say. Partly because we are so prominent within the G7, we continually get invited to euro-area meetings, which the UK would not be part of anyway, because of our G7 mandate. At the moment, I don't see any diminution there. We work very closely there. I think the challenge on why G7 not G20 is there is a cyber element to the operational resilience space, not the whole thing, and that often predetermines the circle of trust, which essentially brings us to certain countries not others. That work is very close—we ran a G7-wide exercise for the first ever time where we worked out how we would co-ordinate communication and other things. I am reasonably pleased with

that. For the global companies, unfortunately their business is beyond the G7 and we do need to make some progress in the G20.

Alison Barker: We work with Lyndon on the G7 and support the work of the various groups on that. Lyndon joint-chairs a lot of that work. From a securities regulator point of view, there is the IOSCO work that we have worked on. We have not seen the requests for us to help or work on the IOSCO side diminish at all. In fact, I would say—I think this is something that Lyndon said at the beginning—we are largely seen in the lead in terms of the thinking and the ideas that we are putting forward. We are not seeing a diminution in that at all.

David Bailey: I would agree with that. When it comes to putting that policy into practice, we have very much been at the forefront of international co-operation with respect to the supervision of individual firms and infrastructure. In my space, we were the first authority to establish global colleges of supervisors to look at some of the infrastructure, the clearing houses that we supervise, and we leverage off expertise in other authorities to help us in some of our assurance work as well.

Q232 **Alison McGovern:** Thank you all. In evidence to us from your organisations, you say that two thirds of IT failure incidents are from retail banking. Is new technology causing harm to consumers?

Alison Barker: One of the things about the statistics that show that two thirds relate to retail banking is that the payment services directive, when that came into place in January last year, introduced certain reporting requirements, so we have a huge increase in notifications in relation to the payment services and often the thresholds for those can be reasonably low. So 65% of the reporting is in relation to retail banks. We have a run rate of about 71 notifications a month, of which 38 would be payment services directive-related notifications. That is the point I would make on the statistics.

On the change, the point to note is the one that we have discussed already a little bit, which is the amount of change, the amount of applications and the expectations of consumers around what they want their banking services to offer them. We have seen an increase and more applications and more things being added, and so we do see an increase of those.

Q233 **Alison McGovern:** I am trying to get to the nub of the issue here. Are we importing risk that could cause harm to consumers by the demand for those new functions?

Alison Barker: No, I think it goes back to the point that we expect firms to understand and manage the change and understand the business services, and understand what the impacts of any outages should be. In our business plan, we have said that we are trying to understand a bit more about what the underlying causes of the statistics that show that change is happening are. We haven't got to the bottom of all of that yet. That is still to report.

Lyndon Nelson: There are two parts to your question, really. On the technology itself, I don't think so, but clearly, there is an element of it driving change. I will give you an example. Some of the more fleet of foot FinTech companies may be changing their banking app three or four times a week. If you are a large retail bank in the UK, you are probably dealing with legacy systems. For competitive reasons, you are probably thinking, "Oh, they have just added that feature in that particular app; we have to do the same." The question that chief IT officers are thinking is, "How many times can we change our app in our week without it falling over?" The question we then come back to is, "How can they manage the change?" If their business depends on their banking app reflecting the latest features, they will have to build a change organisation that can cope with that, and they are up against very agile technology companies. I don't think the technology itself is causing an issue.

Q234 **Alison McGovern:** To come back to the statistics and data, would you say that over-reporting or under-reporting is a bigger problem?

Alison Barker: We still think that we have overall under-reporting. When you think about it across the financial sector, if 65% of it is retail banks, we have under-reporting in other sectors. That might be where we would be thinking. Overall, we think there is under-reporting.

Having said that, the payment services notifications have seen an increase. With the greater awareness of firms that they are supposed to be reporting, we have seen an increase. Our stats this year show 853 notifications in the financial year 2018-19, which is a huge increase on the previous year. That is as much due to a combination of payment services and awareness of firms to notify. That trend is continuing. In the first quarter of this year we are at 191 notifications. That is roughly on track to match the previous year. Overall, we see under-reporting, not necessarily in retail banking, but in other sectors.

Q235 **Alison McGovern:** So you still think that we are dealing with under-reporting rather than over-reporting?

Alison Barker: Yes.

Q236 **Alison McGovern:** That is really interesting. Would any of you support the publication of firms' incident data, or other information about their system robustness or availability, with the idea that consumers ought to be empowered by that knowledge?

Lyndon Nelson: There is standardised reporting on technology, which we got through the industry, so they do currently publish some of that. I am sure it could go further. I am interested in your thoughts on that. There is something already standardised about availability stats. The other thing that we are looking at is the call from the French presidency of the G7 on data that we can compare, so that people such as yourselves can compare how we perform against other developing countries. We are working on that, but I think there is already something for consumers.

David Bailey: Can I just add to that? There is a variety of forms of statistics. For example, on the infrastructure that I supervise in our Annual Report every year, we publish the operational availability of the systems

that we supervise, to make that public. In terms of what is disclosed, we need to think quite carefully about how much information is put into the public domain. It can be helpful if consumers can compare availability and functionality, but if you have cyber incidents, you do not want to publicly reveal vulnerabilities in the system, so we need to be careful with what we think about publishing.

Q237 **Alison McGovern:** That helpfully leads to my last question, which is about communication back to firms. Clearly, you all have a strategic overview; you can see commonalities in a way that individual firms cannot. How do you aid the sector in understanding those commonalities and the strategic issues? I know that lots of conversations happen in and among different firms, but what role do you all play in communicating that to the firms?

Alison Barker: That is a really key question. For example, we have had two big publications over the last year. The first one fed back responses to an assessment and survey of 296 firms on their technology and cyber resilience readiness. It covered things such as how they felt about governance and how they secured their core assets. We compiled that and fed it back to firms through a publication, because it enabled them to see across sectors whether some sectors are different to others. It drew out the point that smaller firms are often less confident about dealing with fibre. It had practical suggestions about the sorts of things that firms can do. We also ran cyber groups. We have 175 firms across the different sectors, which are then grouped together in groups where they can talk and share their ideas, views and thoughts.

The groups came up with their practical suggestions of things that had helped in their sectors and we published that. Again, it fed back the detailed things that firms had tried and that had worked. So, much of this is about what works for firms and what firms find works within their own environments, and then how do we communicate that and explain that more broadly? As I say, those are two examples of where we have done that work and publicised it. We have a page on our website that is about cyber, so firms can go there and get that sort of information.

Lyndon Nelson: Things I would add? Well, we are very keen on the FCA initiatives, because they cover a wider patch. We publish the reviews of the CBEST—this is an ethical hacking test that we did. And then the other thing that I would comment on is that the industry itself is increasingly co-ordinating. So they have an initiative at the moment whereby the industry is sharing information, often with the national cyber-intelligence groups as well, so that they can essentially share information on at-the-minute attacks and trade that all.

So, I think there are a number of ways whereby people will go and try to get this information now, because, as your question implies, it is a very good public good to get this information out there.

Q238 **Chair:** Alison McGovern has talked about preparing, or instant reporting. I want to ask about preparing for incidents and also managing incidents. Mr Nelson, you talked about the G7 exercise, so perhaps you could just

talk us through what exercises or scenarios you each run? I don't know whether you do them together—

Lyndon Nelson: I think we all do it together.

Q239 **Chair:** Right. Whoever is the right person to do that could speak, say who is included, whether it is mandatory, what have you learned—all those sorts of things.

Lyndon Nelson: We can start with the G7, because I think that, in a way, what we did was that we nested that. So essentially, we came up with a cyber-incident that spread from parts of the G7, eventually across. That was testing protocols, communications, how we would deal with issues and how do we inform people about the tools that we would use.

Some countries, when they ran that, also included their industry at the same time. We chose not to do that, because we essentially ran the same scenario in what we call our simex—simulation exercise. We ran that in November last year. Again, that was a major cyber outage, and that included also some extra homework for the firms to think about, should a large, globally significant firm also be incapacitated.

So we run those. The other things that we run, because it is all about capabilities, is that we tend to run slightly more—sorry, you asked how many. About 70 banks, insurance companies and other companies, and FMIs were involved in the simex. Obviously, there were the eight jurisdictions in the G7, because the EU is one. And then there were many parts—I think that something like 300 staff were involved on the day. So these are quite major exercises; it takes something like one year to prepare.

We also do desktops, so we did a desktop with the US Treasury Secretary, where we go through some of the issues that principals—the Chancellor was there—might face. So we do a number of those.

We're always running exercises, in effect, because I think we learn the most from those, and they set the agendas for the groups.

Q240 **Chair:** How many exercises do you run?

Lyndon Nelson: I haven't counted, but I would say at least 10 of some kind or other—

Q241 **Chair:** And is it every couple of months? Is it a programme, or is it—?

Lyndon Nelson: It's a programme, yes. And the G7 has also now accepted that they will be doing a G7-wide programme as well. So we have two programmes to run.

Q242 **Chair:** Is there a role for firms themselves? Do you ask them to run their own internal scenarios?

Lyndon Nelson: Yes. I think that is essentially how this develops. If you think about it like plotlines, we might develop the main plotline and then they can develop sub-plots and run them themselves. Some firms do that extensively. When we are building the scenario, we involve the firms quite

extensively, because we are trying to build. What is the reaction? What sort of issues will we face? So we involve them and it is a joint exercise by the industry and ourselves, although we—

Q243 **Chair:** Do they get quite carried away? Do they come up with creative scenarios?

Lyndon Nelson: Some do, yes. Also, one of the things that we have introduced the last couple of times has been a social media simulator, which I think has been quite an eye-opener. I think one of the weaknesses of the earlier exercises, and David highlighted this earlier on, was that in real life the communication is a very big issue. In exercises, my experience pre-2016 is that people tended to underestimate the effect on comms, but I think that once you have a simulated Twitter feed and other things like that, then I think it got much realer.

So people can get carried away on that, but I think it's all to the good. We always learn a lot of lessons, and as David said we always learn that the communications could be better.

Q244 **Chair:** What happens to the lessons? How does the debrief work? How do you go back? What will you do if you identify an issue?

Lyndon Nelson: We issue a report. I do not quite know where we are in the publication—I signed it off last week, so it should be published soon. That will have within it a number of work programmes—we will look at one on data integrity, and one on what we would do if a major institution was incapacitated. We are looking at communications. We will be quite open about that. We will obviously talk to individual firms as supervisors, and about how they would deal with an incident and what actions they need to take. We have supervisory programmes for a number of firms that need to improve, and we make maximum use of that.

Q245 **Chair:** If they need to improve, do you have a timeline for them—there are this many weeks or months, or something, to put something in place?

Lyndon Nelson: Yes.

Q246 **Chair:** We have been talking to firms a lot and gathering evidence, and they talk about a convenor role for regulators and about firms helping each other out—the idea of a sheltered harbour when something happens. We hear a lot that firms cannot even work together to come up with joint banking when banks have pulled out of high streets. What is the likelihood of them coming up with something? We must also maintain data integrity—I think you mentioned that earlier, Mr Bailey—were there to be a significant incident in a major front-facing financial institution.

Lyndon Nelson: The US provides a good model—that is where Sheltered Harbor comes from, and there are a number of other initiatives where firms are getting together. The UK industry has been a bit behind, but I think it is catching up. Like you, I think we will have to wait and see to what extent firms can achieve full collaboration. In a way, they sort of have to. In many ways, for financial resilience, the Central Bank has a number of tools it can use with the right will. If a firm the size of Barclays

or HSBC said that our retail banking system isn't working, there is nothing the Central Bank can do.

Q247 **Chair:** Because it is just so big with so many customers.

Lyndon Nelson: Exactly. The industry has to work together. It is early days, but there are promising early signs that firms are getting together and working on those things. They have some definite advantages. Some are more evangelist about this thing than others. For example, we know that some firms have people on their payroll who are there simply to help the sector work. They are not arguing for the characteristics of a particular firm. Those are all good signs, but it is early for the UK.

David Bailey: We have seen some signs of incidents where firms, or the infrastructure, can reroute the way they do things. For example, if an individual bank faces an issue with one payment system, it can reroute its payments through another one. If one payment system is down, industry can direct payments through a different pipe. There have been good examples of that collaboration taking place, and we can build on that.

Lyndon Nelson: Those examples come from our exercises—we have shut one payment system down, and firms then look for alternatives. We then think, "Okay, that seems feasible. How can we make that alternative work properly and with minimum risk?"

Q248 **Chair:** What are your respective roles when there is an incident? Let's take TSB, for example—there was a lot of interest in that in spring last year. I don't know whether that is the right example to use, and there might be others, but talk us through it. Perhaps the PRA could start—when there is an incident, what does the PRA do?

Lyndon Nelson: I am still wearing three hats here. I manage the specialists. We put specialists into the institution—Alison can talk about that. Then I supervise and take decisions on safety and the soundness of TSB. My additional role is to convene the authority's response framework, so where we believe there may be an issue—

Q249 **Chair:** Could you talk about that?

Lyndon Nelson: Yes of course. That is principally the Treasury, the Bank of England and the FCA. Essentially, we co-ordinate episodes that may need that collaboration.

Q250 **Chair:** Is that for episodes that are a systemic risk? Does it depend on size?

Lyndon Nelson: A few years ago the answer would have been yes, but we have lowered the call threshold for cyber incidents—Alison alluded to this earlier on—because they are so complicated, and there are a number of hypotheses about how they may turn out. We have effectively lowered the escalation criteria so that we summon them earlier. Yes, if it is called, it is not necessarily a financial stability event; it is just one that may require some co-ordination. We would be co-ordinating with that. The chair of that group will move according to which authority is likely to be

most in the lead, but we effectively run the secretariat for that. Those were my three roles within the TSB.

Q251 **Chair:** With TSB or an incident such as that, what is the FCA's role?

Alison Barker: Often we are the first responder, because often how an incident will develop is that either an institution will call us to say that something has happened, and it will have a significant impact on customers, or we see that developing on social media ourselves. We have social media monitoring that we use anyway, so we monitor in real time what is happening on social media for the banks. If we see an incident starting to develop, we might ring a bank and say, "What's going on?", if they have not rung us first.

As the first responder, we will establish the facts of what is happening and establish the key point of contact within the institution. We will inevitably contact the Bank and the Treasury. There will then be the co-ordinating authorities call, which will have a set agenda around ensuring that we know what is happened, that we understand the impacts, that we know who is doing what at the firm, that we are clear that the firm understands what it has going on and what level of response we need to have. In the TSB incident that you mentioned, we quickly established that we needed to have both PRA and FCA staff on site to monitor the situation, including two senior advisers from the FCA. Those are our very senior people.

Q252 **Chair:** So you have those people on stand-by to go in?

Alison Barker: We have people on stand-by, but from the FCA point of view, because we are the first responder, we will be monitoring things and we have teams on call over every single weekend and over bank holidays to monitor incidents. If something happens on a Saturday afternoon or a Sunday, we have staff on call and available.

Lyndon Nelson: It is usually a Friday, isn't it?

Alison Barker: It is usually a Friday. All incidents start on a Friday. We will co-ordinate, and for the specialists we run staff on a rota over every single weekend and bank holiday, particularly at high-volume times such as Black Friday, where there are high internet shopping-type things. We will particularly monitor those. We will co-ordinate the response. As Lyndon mentioned, if it becomes a safety and soundness issue for a particular firm that is dual-regulated, the Bank would take over the chairing of the co-ordination call. If it was a much bigger stability issue, I think the Treasury would take over if it required bigger co-ordination.

We are well practised in what it is that we need to do, how we need to work on those incidents and what we need to focus on. The key area that we have focused on, which we have talked about a lot, is communications, particularly to consumers. In the TSB incident we had three core objectives that we needed them to meet. One was about how they were communicating with consumers, two was about how they were dealing with recompense and redress and the third was how they were responding to and managing vulnerable consumers.

In an incident, they should ensure that call centres have enough people there, for example, and that the people in the call centres are thinking about responding in an appropriate way to people who are ringing up and saying, "All my money's gone." We need to ensure that we are thinking through those types of things and ensuring that firms are responding appropriately.

Lyndon Nelson: If it is a cyber incident we will include the NCSC and if it is criminal the NCA, so they are all involved.

Q253 **Chair:** They are all on stand-by.

David Bailey: The TSB example is less relevant from my own perspective, the infrastructure perspective, although we were involved just in case there was any need to—

Q254 **Chair:** Visa, I suppose, would be the example.

David Bailey: That was the example I was going to come to, where we were the lead authority, because it was an incident that was affecting a huge number of people in real time. We led the authorities' response to that one, co-ordinating in much the same way as Lyndon and Alison have outlined, but also including the Payment Systems Regulator, which has a specific interest. The one additional point I would make on infrastructure is that, if there is an issue at an infrastructure, by definition it will have an impact on a wide range of firms, so there can be a more pressing need to get the industry together to ensure that communications and responses are being co-ordinated.

Q255 **John Mann:** Do you have the expertise and do you have the resources to deal with the potential of state-sponsored cyber-attacks, either from rogue states or from superpowers, should that happen in the next few years?

Lyndon Nelson: We do and we would rely very much on the NCSC. We don't have those sorts of resources in supervision. Clearly, the Bank of England would also be a target in the scenarios you highlight. We have experts protecting the Bank's systems and we work closely with them if we need to, but in the scenario you highlight we would be very dependent on the NCSC.

Q256 **John Mann:** As I contemplated it, it was targeted at the banking and financial services sector, as opposed to anything wider.

Lyndon Nelson: We were subject to the CBEST penetration test, too, and that highlighted some vulnerabilities. I won't go into those, for obvious reasons. We have been fixing them; I think our chief operating officer gave evidence to another Committee saying that she felt there were no vulnerabilities there. I think that is where we would be, although as you highlighted, it is very difficult.

Q257 **John Mann:** I am trying to be reassured or not depending on whether, in your judgment, you have the expertise and the resource. That is something we can attempt to influence, if you have not. We wouldn't want to find out about that afterwards.

Lyndon Nelson: You may need to call others to give evidence as far as the Bank's resilience is concerned. I know from a matter of merit—senior management are obviously involved in these things, because we look at the standards we apply—the Bank has put a lot of investment into it and it is a very impressive process. As you describe, nation states are pretty effective actors in these things, so one always has to be careful.

Alison Barker: The only thing I would add is that we work very closely with the National Cyber Security Centre; they provide a level of support in terms of threat assessment and focus, and we have talked a bit about information and intelligence sharing. Our view would be that they are very much on top of that agenda.

Q258 **John Mann:** So within the organisation you have sufficient expertise? My fear would be that you are relying on others with expertise; you don't necessarily have the expertise even to be able to really ask the difficult questions of others.

Alison Barker: Their role is very much to identify when things might be coming our way; that is a key part of it. We don't have the expertise to identify when things might be coming our way on cyber. They would do that.

From the FCA point of view, we have estimated that we can run at least 10 incidents at the same time. We are resourced to do that and the system that we have enables us to do that. The incident response management is our core role at that point, across something that has happened. It's how we are able to respond and deal with that.

We have really upped the game on the amount of work we have put in over the last two to three years to bring awareness to firms about their role in identifying their own cyber-security measures. The point about firms being able to both spot incidents and protect themselves put the emphasis on respond and recover; we know how they are managing an incident. As regulators we have put a lot of work into that in the last three years. We would say that firms are much better prepared than they were three years ago to deal with the types of incidents that you were talking about.

Lyndon Nelson: The penetration testing that we have been talking about—the CBEST—has the full title "threat-led penetration testing." It fundamentally relies on either the NCSC or an NCSC-accredited provider, regarding what the threat might be. We have tested 34 firms, including the Bank, on those measures. For all firms there were some actions, but you can be assured that the threat that we assessed at the time was precisely the one that we tested the firms on. That combination of skills, either from the industry—because we use accredited providers—from the NCSC and from supervision, can give you a reasonable level of assurance, but I could never stand or sit here today and give complete assurance, given it is a constantly changing environment and constantly changing threat.

Q259 **John Mann:** Obviously. I would simply make the point that if you feel that you do not have either the expertise or the resource, it is incumbent

on your organisations to inform Parliament—be it in a public session, or discreetly to the Chair of the Treasury Committee. On behalf of Parliament, this Committee would regard that as absolutely essential.

Chair: Yes.

Lyndon Nelson: I would add that the PRC has a legal obligation to report every year on the adequacy of resources, and this is one of the questions that they ask.

Q260 **John Mann:** The number of IT incidents affecting financial services consumers is going up. Is it going to continue going up?

Alison Barker: The thing we talked about is the incidents reported and whether we have under-reporting. In some ways, I might want to see the incidents reported going out, to—

Chair: To make sure it is more accurate.

Alison Barker: To make it more accurate in terms of the reporting levels. I think you mentioned at the beginning what we would expect the outcome to be from the CP and the work on that. Again, we would expect to see firms being much more aware of their business services and the impact on their consumers. When we talk about operational resilience, we are not talking about zero failures. The outcome for consumers means they can still access services, but it might be a different one—if telephony services are down, for example, they can operate through internet banking or mobile banking. It is not that the whole thing ceases to act and causes consumers not to have access to services; it is about how outages are managed.

Q261 **John Mann:** How much is it inconvenience to consumers? If my train is delayed because of some technical problem, it is a great inconvenience. How much is it harm? If I am stuck in this weather for 24 hours, it might be slightly more than inconvenience for someone of my elderly age. When it comes to financial services, do you have a definition of inconvenience versus harm? Is there a difference in your view?

Alison Barker: From a harm point of view, the sorts of things we are focused on—I am thinking about the definition of vulnerable consumers. If a service is not working in the way that is expected, the harm might be that it causes quite a great deal of stress for vulnerable individuals. Yesterday we published our consultation on how firms should think about dealing with vulnerability, which is very important in an operational resilience sense. Having a single definition might not take into account vulnerability, so we want to be mindful of that. The types of harms that we have seen include the Tesco Bank incident that affected Tesco customers, and we have issued a final notice on that. People were recompensed in the end, but they lost money over that weekend, which is a very stressful situation for consumers to face. Likewise, with TSB people could not access accounts and pay bills. Those are actual examples. I would not class them as inconvenience; people really did suffer.

Q262 **John Mann:** Do you think there is scope for more clearly defining harm? Where there is harm, the speed of response, and potentially the redress, is more important.

Alison Barker: Yes.

Lyndon Nelson: That is possibly where the impact tolerance work will go, because that might define your threshold. Your comment about the response is interesting. Some of the firms we supervise are insurance companies that insure against data loss. They offer their clients an additional service, which is managing incidents, and one of the interesting things they find is that if an incident is managed properly—there is proper communication to consumers and all of that—it leads to something like 30% fewer losses, purely in accounting terms; I am not at all underplaying the stress amount. That shows that firms that are properly organised and think about a plan B and their responses can deliver tangible reductions in harm.

You are quite right. We have talked about impact tolerances—we have typically defined this as a time period, but we have also left it open and it could be other factors. That is obviously down to the particular regulators and what their objectives would be, but it may well involve, as Alison said, a vulnerability lens and another type of lens and not simply an amount of time. It could be volume; it could be something else.

Q263 **John Mann:** I don't know whether TSB was, in your judgment, at risk of collapse, but my final question is about consumer or customer response post incident. We have not really seen yet a mass panic response in this country, but I can perceive plenty of scenarios and behaviour where there is—where the word gets out and it spreads like wildfire: "Get your money out of this institution." There was an element of that with TSB.

Mr Simon Clarke: With Northern Rock, we got pretty close.

John Mann: And Northern Rock, with people queuing. One could see this in the future. How thought through is the system for dealing with it and for trying to militate against what almost certainly would be irrational behaviour by people, acting in panic because everybody else was? We are very British: if there's a queue, people join it.

Lyndon Nelson: And work out what it's for at the end, yes!

John Mann: One could see this at some stage, at any stage, becoming something of a crisis, but that could be avoided if systems and procedures were thought through enough.

Lyndon Nelson: It is a real issue, Mr Mann. At the Basel Committee, we had a presentation from one of the other countries that highlighted precisely the type of incident you describe. There were some issues with a particular local bank. It was in a relatively remote part of a very large country. Through social media, effectively, the bank had a massive liquidity run on it. We have seen some instances; we've had the odd social media issue within the UK.

I think one of the ways we would respond to that, in terms of the issue that I am interested in—the liquidity of the firm—is that we may have to think again about how sticky deposits are in those circumstances. Are they going to be much more liable to run than we traditionally have assumed that they might be? We may have to recalibrate liquidity. Simply put, they may have to hold more liquidity for those things.

I think your other point is very well made. This is why we have emphasised communication as one of the key planks of the discussion document. Managing the incident becomes incredibly important, and at the very least we don't want people adding fuel to the fire unnecessarily, but how we cope with that in a social media age is a very real challenge. The Basel Committee is looking at recalibrating the liquidity policy, because of just that one incident. It's early days, but we are looking. And then we are thinking about communication in our own domestic setting.

Q264 **John Mann:** I'll just sneak this one in; I've got to ask this. Mr Bailey, you are very quiet at the moment. In this scenario, will it be the Governor who goes on TV to reassure the population, or will it be, let's say, the Prime Minister?

David Bailey: That's a great question—I wish you hadn't asked me!

John Mann: Well, could one anticipate that the Governor would be taking the lead—would be the public face—in this?

David Bailey: That comes down to, I think, some of the co-ordination mechanisms we have talked about. Lyndon has talked about the authorities' response framework. Amongst us as we are dealing with an incident, we are very clear about who is in charge. Depending on whether it involves consumer detriment, financial stability or even a broader issue, that will dictate who is actually taking the lead on it. As part of that, we will have a great focus on communication, which we have touched on many times during this session. Depending on the incident, you will see the authorities saying things, and you will see the most senior people in those authorities saying things if necessary. It would depend on the specific incident—whether it is a continuing detriment issue or a financial stability issue. That will determine what we say and who says it.

Lyndon Nelson: In the exercises that we run, we absolutely contemplate asking the Governor, the Chancellor or whoever to do these things, because that is what we think is the right response at the time.

Q265 **Mr Baker:** What is the role of legacy systems? To what extent are legacy systems being used across the sector?

Lyndon Nelson: Still pretty extensively, I'm afraid—partly because often the industry has grown up through organic merger, and those legacy systems are there. Some pretty core systems are still run on legacies.

Q266 **Mr Baker:** Are mainframes and COBOL things that people don't—

Lyndon Nelson: They still exist, yes. I gave a speech last year—I think there is still code back from the 1970s on some of these systems, and they have just built on top of it.

Q267 **Mr Baker:** To what extent do they have plans to phase out old COBOL mainframes?

Lyndon Nelson: I think they do have plans. It often takes quite a brave chief technology officer to envisage that, but as I described earlier the competitive pressure that some of them now feel, being up against these more agile FinTech-type companies, means that they are going to have to leave the legacy systems behind. A number of these improvements are to do both—to remove the legacy and make it more agile.

Q268 **Mr Baker:** Do you have any examples where either the age or the complexity of systems has inhibited the ability of banks or institutions to comply with new regulations?

Lyndon Nelson: I do not. I think the RBS outage in Ireland was largely down to a legacy issue. Of course, within that outage they failed to meet a number of regulatory requirements at the time, but I am not aware of a legacy causing an issue of compliance.

Q269 **Mr Baker:** We have statistics that tell us that change management is the principal cause, and you are agreeing. Do you think that it will become more or less difficult as time goes on to deal with change management issues around mainframes and other legacy systems?

Lyndon Nelson: I think it won't change. What will change, though, is the demands on them. They cannot carry on with the legacies and the approach that they have, because I think it would become a front office business issue about them not being agile enough, when consumers are demanding those things.

Q270 **Mr Baker:** So they cannot carry on with those very old legacy systems.

Lyndon Nelson: That would be my conclusion, and I think a number of the firms themselves have reached that conclusion as well.

David Bailey: This is where accountability for the resilience in the firms' operations comes in. As part of the discussion paper, we are very much holding boards accountable. Also, both my colleagues at the PRA and the FCA have the senior managers regime, where they can place specific accountability on individuals to be responsible. That will include, for example, understanding what risks are being run by legacy IT systems.

We do not have that same senior managers regime applicable to financial market infrastructure. In fact, that is something that the FPC called out in the most recent financial stability report. It is an area where accountability in the firms that I supervise could be enhanced, if we had a common approach to the senior managers regime.

Q271 **Mr Baker:** Do you think that firms are investing adequately to deal with these legacy systems?

Lyndon Nelson: Adequate is difficult. They are putting a lot of money into it, I would say. We are slightly torn because, of course, as you pointed out, change makes them vulnerable. You do not want it to be too rapid. At the same time, you want the removal of it. We have not taken any regulatory action about it being inadequate, if I can put it that way.

Q272 **Mr Baker:** Do you share my concerns that the longer people go on running legacy systems like mainframes running COBOL, which people do not learn any more, the more difficult it will become to deal with change management on those systems, and the more the chances will increase of failures?

Lyndon Nelson: It would, for a simple demographic reason: how many COBOL programmers do you know and how many are going to be left?

Q273 **Mr Baker:** We are talking about senior managers' accountability and about investment. What message would you want all of us to take to the industry about legacy systems, and their resilience and their capacity to serve customers?

David Bailey: Part of it would be having a very structured approach to understanding where the risks are, and what the timelines are for those systems to either become obsolete or the risks to increase, and having a clear plan for their replacement or renewal. If I look at the payment sector, for example, that we supervise, we have a significant number of infrastructure projects going on. The Bank itself, for example, is replacing our own real time gross settlement system. That is not saying our existing system is out of date. It is perfectly fit for purpose; but we know now that we need to be making the changes now so that it is fit for purpose for the next 20 years. We will be expecting individual institutions to be thinking ahead of the curve, rather than getting a system that is out of date and then thinking about how to replace it.

Q274 **Mr Baker:** We talked earlier about code from the '70s. I was born in '71 and I am 48, so we might have code that is getting on for as old as me. Another 20 years—my goodness. I will be retiring and yet my bank account could still be run on a mainframe that is older than I am.

Lyndon Nelson: I am hoping that the discussion paper, when we make it to policy, will effectively eliminate that; because, if you think about it, the firm will have to think about what services to provide to the consumer, for example, and what is in the production line to get that service to them. Our best estimate is that, if there is a legacy system in there, their response time or their recovery time is going to be a lot higher. So the policy, I think, is going to drive out that. Let's hope. Let's have an ambition, however modest, that when you retire maybe there is no—

Q275 **Mr Baker:** Would you be more ambitious than that and say that they for example ought to get rid of certain legacy systems within, say, five years?

Lyndon Nelson: Well, I am ambitious on the outcome. I am ambitious on delivering an outcome for customers, and if that involves getting rid of legacy systems I am all for that.

Q276 **Mr Baker:** That is partly about leaving them free to make a choice which suits them.

Lyndon Nelson: I think that is commensurate with the responsibility they have to take—

Q277 **Mr Baker:** So, looking at their broader capacity, how confident are you that institutions do have the capacity to improve their change management?

Lyndon Nelson: Clearly, from the stats, there is still some improvement to be done, but the industry, certainly the big banks, in terms of structural reform that was a very major IT project and they did carry that out to a very high standard, I thought. So I am hopeful that it can be done, but of course they have pressures on other issues, too. So clearly it could be better, and that is what the occasional discussion paper is for, but we have had good evidence that they can do it.

Q278 **Mr Baker:** Would you say that their risk management approach is adequate to the consequences of getting change management wrong?

Lyndon Nelson: I think there are a number of weaknesses in risk management. It is a bit like the comments that other Members have made around expertise. So you need expertise on the frontline. You also need expertise in risk management. We have a number of remedial programmes about that, so I think we could see an improvement in risk management.

Q279 **Mr Baker:** Turning to mergers and acquisitions, which could involve institutions both of which had very old, complex systems, perhaps not well understood even by their own staff sometimes. You seem to be agreeing. How confident are you about firms' capacity to manage systems integration during mergers and acquisitions, when possibly both of them have legacy systems?

Lyndon Nelson: Again, we have evidence of it not working, but actually probably the majority of it working quite well. So, the amount of change that goes on—there is only a very small percentage. It is obviously something that we look at very carefully, because of our objectives. I know Alison looks very carefully because of hers, and David, too. So we do look at these things very closely. Often, I think some of the synergies and the benefits of the merger are in taking out some of those costs, so management of firms are equally focused. We do have to make an evaluation of that.

Q280 **Mr Baker:** Have you ever, or do you think you could ever decline a merger or acquisition because of concerns about operational resilience?

Lyndon Nelson: We have, and we would.

Q281 **Mr Baker:** Just in closing, I am just struck that, as I was saying that some of these systems are not well understood by their own staff, two of you on my right agreed with me, nodding. I am just slightly concerned. It is not catching you out, but members of the public would probably be alarmed to think that some of their financial institutions are running on systems which are possibly 50 years old, almost, and which possibly, or probably—I have got enough experience to know—are often not well understood or perfectly understood by people working with them. How widespread is that problem? Are we really in a world wheresoftware systems are not perfectly understood, in—is it in most or a tiny minority of institutions?

Lyndon Nelson: I think it is a question of degree. I think they do understand them, because they build things on top of them. Often, I think, the understanding is deficient when something goes wrong with them. That is the RBS case, I think, in the Irish outage. It was fine to build things on top of it, but—

Q282 **Mr Baker:** I recognise I have only worked at a small number of institutions, so my experience might not be representative, but I suppose what I am asking you is whether you think it is representative. Do you think the software systems of financial institutions are not well understood—or not perfectly understood, let's say—by their own software engineers? Perhaps you would like to come in, Mr Bailey.

David Bailey: Yes, I was going to. That is exactly why, on the back of the discussion paper we published, when we take our policy forward later this year we need firms to identify the critical services and the systems that support those services. It may be that there is some very old technology sitting inside a firm—whether that is a bank, an insurer, an investment firm or the type of infrastructure I am responsible for—but it is not linked to the critical business service that matters to the customer, whether that is a retail customer or a wholesale customer. By taking our approach forward, we will get clear evidence from firms that says, "This is the service that matters, these are the systems that underpin that, and these are our views on those systems." Subject to us taking the policy forward, next time you ask us to come along, we will be in a better place to answer that question.

Q283 **Mr Baker:** I am reassured. Thank you very much.

Alison Barker: Where we have looked at the change management stats and gone through them to understand the root causes, when we have come to legacy systems, one of the points—the one Lyndon made—is that the systems sometimes are not well understood. There is a broader question, which I am not sure we can answer right across the piece, but when we have dug into the evidence about what has happened on a particular issue, the cause has sometimes been that a particular system was not understood, or it was an old system that could not be patched, so patching had become a problem.

Chair: I like the way Mr Bailey volunteered himself and the panel to come back before the Committee. Most people do not do that when they are sitting in a session, but we welcome it very much. I should have said before that, unfortunately, I have to go and sort out a constituency issue, so Mr Mann is going to chair the last couple of sections. Thank you very much for your time this morning.

In the absence of the Chair, John Mann was called to the Chair.

Q284 **Rushanara Ali:** I want to pick up on the issues with companies that have had IT problems—Lloyds TSB, Visa and others. Perhaps this is a question for Ms Barker. One of the things I am very concerned about is that it takes a very long time for consumers to get redress. There is still an investigation, and we still have not had the report about what went wrong. In the meantime, we are in the dark about whether our

constituents have had the redress they need. The financial ombudsman gets referred to quite a lot. They have a hell of a lot to do and, frankly, people can wait a very long time before problems are rectified. We heard horror stories of what had happened to people.

In the light of everything you have said, how confident are you that if problems arise in the future—they are bound to, given the increasing reliance on technology and so on—the plan Bs that firms have in place take into account sufficiently the fact that action needs to be taken for consumers to get redress immediately? Otherwise, things just go on and on, and then get forgotten about.

Alison Barker: If we are talking about the TSB incident, I would just separate the joint investigation, which is ongoing, as you rightly say. That will take a path to conclude; that has not concluded yet. But in relation to that incident, the published information is that 204,000 complaints were received, 90% of which have now been resolved, including reopening 86,000 complaints that were received before October, and customers have received redress. It is possible that you have constituents in that last 10% that have not been concluded yet, but we are very focused. One of the three key objectives we had around TSB was ensuring redress for consumers, and yes, we want to ensure that there is speedy and appropriate handling of complaints.

Q285 **Rushanara Ali:** We should expect some very clear standards setting out what timeframe consumers should expect for complaints to be resolved, rather than an inquiry taking place. It is quite a long time since it happened.

Alison Barker: Yes.

Q286 **Rushanara Ali:** Obviously, you don't need to go into the specific timelines, but I suspect it will be some time, from when the problem started, for the 90% or so you mentioned to get their issues resolved. Our Chair referred to a case at the time that was pretty shocking and, frankly, an insult to the experience that people had. I would struggle to call that compensation. It would be helpful to get more, perhaps in writing, on whatever you can tell us ahead of the inquiry findings coming through.

Alison Barker: Of course.

Lyndon Nelson: I have a couple of things to add, if I may. Plan B is aimed at reducing the harm at source. The Chair mentioned Sheltered Harbor. One of the challenges we will have is data corruption. If the data is corrupted, we will face a challenge of timeliness, about whether both sides are happy with what you had on deposit. Sheltered Harbor is interesting; it solves a number of issues but not others. One of the principal things it is trying to help with is to reassure retail consumers that, for example, "We know, Ms Ali, that you have £3,000 on deposit—don't worry about." That is deliberately designed for that. That is why data corruption will be important, because it will lead to delays for constituents while we try to sort it out, unless we find a better solution.

Q287 **Rushanara Ali:** Moving on to data and resilience, is that the aspect of operational resilience of firms that concerns you most?

Lyndon Nelson: Yes. You have had evidence from one of our financial policy committee representatives that the data integrity issue is the one. In terms of the solutions that we would have to put in place and how long it would take to rectify, that is probably the one that we would fear the most.

Rushanara Ali: How long?

Lyndon Nelson: That depends on the nature.

Rushanara Ali: Give me a range of what you think.

Lyndon Nelson: It could be months.

Alison Barker: On the data integrity bit, the point you made is how the impact on consumers is handled. All that needs to be explained and communicated. The knock-on effects that need to be carefully thought through, as well. That would be an additional part of that.

Q288 **Rushanara Ali:** You mentioned the regulatory sandbox. Could you say a bit more about that and what it would mean? What is its role?

Alison Barker: One of the FCA's objectives is to promote competition. The sandbox is there as a place where firms can come and experiment with innovative ideas and ways of doing things. We take in cohorts of firms; for example, some use distributed ledger technologies as ways of doing things. It gives a safe environment in which the firm can experiment and be closely monitored at the same time by the regulator. It is about fostering innovation in a safe way, which brings benefits to consumers and markets because it brings new things that people can have.

Q289 **Rushanara Ali:** Where does Open Banking feature in that? Are people looking at the downsides and mitigating risks? There have been some concerns about that. Could you say something about the FinTech hub? Obviously, there is more use of FinTech.

Alison Barker: Open Banking is here and with us now. That is about allowing consumers to see data in different ways. We have already approved a number of information service providers.

Q290 **Rushanara Ali:** Are there any risks associated with Open Banking that you are particularly concerned about?

Alison Barker: We are aware of the comments where people say, "If you have access to banking systems, will that create more risk?" We are monitoring that closely. In our statistics of the things that have been notified to us, 0.2% relate to Open Banking. We have not seen any issues coming through, but we are aware of the risks and have very closely assessed the information service providers to make sure that their technology is appropriate and strong. That is the sort of work that we are doing in that space.

FinTech is slightly different. We ran FinTech sprints, which look at whether there are particular issues to solve within the financial sector that new FinTech start-ups could help with. Next week, I think, we are running one on financial crime, looking at different ways of solving some of the challenges within the financial crime space. That brings together groups of FinTech people, and developing ideas and thoughts. We run those on a reasonably frequent basis, and we have run them internationally.

Q291 **Rushanara Ali:** Are you concerned about some technology companies structuring their activities within the financial services sector to avoid regulation? Have you picked that up?

Alison Barker: Not particularly, but we always have challenges with the perimeter and who is on which side of it, so we do watch that carefully. If we have firms doing activities that ought to be regulated, but they are doing them and they are not regulated, we take specific action.

Q292 **Rushanara Ali:** Mr Nelson, you were nodding.

Lyndon Nelson: Yes. The Financial Policy Committee has a legal responsibility, and it looks at that. There are obviously debates at the moment around things like the cloud and others. We are obviously looking at that. David could come in because he probably has one of the few where we have brought something into regulation. Do you want to talk about that?

David Bailey: Yes, I can do—

Q293 **Rushanara Ali:** Before that, will you say something about the cloud, because it came up previously? There is over-reliance on three, is that right?

Lyndon Nelson: There is a limited number. There are a few more, but three by far have the biggest market share, yes. That obviously provides a degree of concentration in the system.

Q294 **Rushanara Ali:** What are your concerns about the reliance on those three? Are there any concerns?

Lyndon Nelson: I always have concerns.

Q295 **Rushanara Ali:** Do we have a parallel with the banking crisis? At some point, banks are over-reliant, and they are in a too-big-to-fail scenario.

Lyndon Nelson: We deal with concentrations all the time. David supervises a number of things that are concentrated in the system. I am concerned about the shortage of choice, but that is the outcome based on the occasional paper. If your constituent is reliant on them for a service, they have essentially to tell us what happens if it is not there. We are looking very closely at the safety of the cloud and in the cloud. For most small companies, it is probably a better outcome for them, because for some of the threats that Mr Mann referred to, the cloud providers are probably better placed to provide protection than a small building society or something like that. It is a slightly more nuanced picture about the cloud providers, but we are obviously worried about the concentration.

Q296 **Rushanara Ali:** My final question is about the overall trend towards reliance on technology, including AI. There is increasing evidence that AI has discriminatory outcomes. An MIT study showed that recognition of white men was only 1% different. Errors around darker-skinned women were about 35%, and some experiments showed that AI could not even recognise Oprah Winfrey, Michele Obama or Serena Williams—so there is not much hope for me in that kind of experiment. What are your thoughts about the increasing reliance on technology in the financial services sector, and whether there is a need for regulation? That is in terms of the previous points about technology—what do we need to do—and how we ensure that consumers are not differently treated. That is a big number. What are your thoughts?

Lyndon Nelson: We are looking at some of this at the moment. There are some positives from it, but you are quite right that the way in which some of the models are established means that they either reflect the biases of humanity or put those in. The important thing for the regulator is that these cannot be a black box. The management need to understand what outcomes they come up with, and the regulator needs to understand those as well. There are a number of techniques we can use to do that. We can essentially put your picture, maybe, with a couple of others and say, "Well, how does it deal with it?" We can run a sort of hypothetical portfolio through that, but equally we need to understand that management understand these things. They are increasingly coming in, but—because of the way the rules are written—very much with this proviso that people have to explain them.

Q297 **Rushanara Ali:** So at the moment, they are not assessing the impact, are they? They are not looking at that, and that is pretty serious. If those are the numbers across the board, you could get quite a dramatic—

Lyndon Nelson: Exactly. This is why we are being very cautious. In insurance, for example, all the biases we have written out in the policy could be re-introduced, so we are obviously looking at these sorts of things very closely.

Chair: Mr Clarke?

Q298 **Mr Simon Clarke:** Thank you, Mr Mann—I love saying "Mr Mann", by the way; it's great—and thank you all. A lot of the issues that we were touching on there with Rushanara and the penultimate question are questions that arise in my brief on concentration risk and how we can mitigate that, and crucially, I suppose, how the regulator can help to address that risk.

Starting from base principles, is there an inherent desirability to insourced or outsourced services that are fundamental to IT? Perhaps, Alison, you would lead off with that. Do you have any inherent presumption about the desirability?

Alison Barker: No, we don't. What we are clear about, which is the point David made, is that senior management of a firm are responsible for understanding what systems they are using and how they work. If they have decided to outsource services or use third parties—all firms use some form of third parties; electricity, telephones, and all of those things are

somebody else's responsibility—they can outsource the activity, but they can't outsource the responsibility for overseeing that it is working and understanding the impact of it when it does not work. That is a core tenet from a regulator's point of view that we stick by.

We try to help. We give useful pointers about what people should do; we will supervise whether there is proper oversight of outsourcers, but in terms of a preference, we do not have one.

Q299 **Mr Simon Clarke:** In terms of what the regulator can do specifically, Mr Nelson, what would be your role in terms of making sure that there is indeed the requisite level of regulation? Indeed, do you interact directly with some of the outsourcing providers?

Lyndon Nelson: We do. Alison describes it: the way you deal with outsourcing is largely to ignore the outsourcer and to have the requirements on the firm. Ultimately, however—David will have this example—we can actually bring the outsource provider into the regulatory network, so those are really the two bits we can—

Q300 **Mr Simon Clarke:** Can and do.

Lyndon Nelson: Can and do, yes. We have had conversations with some of the cloud providers about these things, and the European Banking Authority, for example, introduced an audit access requirement and things like that. We found that quite helpful. As we put it to them, they can either have 50 disintermediated conversations via their clients, which are our regulated population, or they could talk to us, so we have had a better dialogue about that. We have been particularly focused on how firms can exit and enter these contracts, and how much choice they actually have about what contractual terms they have, because obviously they have regulatory obligations and that will matter.

Q301 **Mr Simon Clarke:** Yes, indeed. Mr Bailey, from your side of things at the Bank, are you satisfied that there is sufficient robustness, if you like, in this area, which is in some ways more opaque than the regulation of the banks themselves?

David Bailey: It is really important that we place the primary accountability with the management of the financial services firms themselves, but as Lyndon has highlighted, where we do see some concentration or reliance, we have other options.

To give you an example, the infrastructure that underpins several of the payment systems that I am responsible for supervising—faster payments, Bacs and LINK—is all provided by a single firm, Vocalink. Last year, we took the decision that while FPS, Bacs and LINK remain primarily accountable for the services they outsource to Vocalink, it had reached a significance that meant we needed to recommend to the Treasury that it was brought within the regulatory perimeter. Since last year, we have had a direct supervisory responsibility for Vocalink, so we can think about that.

We can also think about how to expand the regulatory perimeter when activities expand. Again, we recommended this, and the Treasury made a change via the Digital Economy Act two years ago that enabled us to

supervise not just inter-bank payment systems, but payment systems that might operate in a way that facilitated payments between individuals without a bank intermediating them. We have tools that we can use.

Q302 **Mr Simon Clarke:** That's helpful. Both you and Alison have referred to the fact that you cannot outsource the responsibility—you can outsource the function, but not the legal responsibility. One of my concerns is about the accountability of the governance structure surrounding all this. I am thinking about the SMR regime and Paul Pester, who we had in front of our Committee on a number of occasions last year in connection with the TSB crisis. There was no fallout from that, in terms of his fitness to head a bank or be involved in a leading financial institution, despite the fact that he had presided over such a calamitous failure, which had done real harm to a number of customers. Is there concern that the regime does not have sufficient teeth?

Alison Barker: The senior managers regime has placed specific responsibility on individuals. It is across certain institutions at the moment and will be expanded more broadly by the end of this year. We think that has made a difference. On TSB, which you mentioned, the investigation is ongoing, as I have said.

Q303 **Mr Simon Clarke:** It is still potentially that the SMR could yet bite.

Alison Barker: So we have an ongoing investigation there. If we are looking at individuals taking on responsibilities, we do an interview with them. Obviously, it is important to ask those sorts of questions. Governance is hugely important, and we have stressed the importance of the accountability of management for properly understanding what they are doing. I think Andrew Bailey's written response in relation to TSB made that very clear.

Lyndon Nelson: Just one point. I would also say the SMR bites even at pre-enforcement. When we are talking about some of these big programmes that your colleagues have mentioned, one of the big things that the supervisor does is make sure who is responsible. That is in the normal course of business and has been made much easier with the SMR regime.

Q304 **Mr Simon Clarke:** Leaving aside the TSB example, because it is still sub judice, can you cite examples of where the SMR or accountability structures have bitten firms that have not upheld their responsibilities, or is this unchartered water?

Lyndon Nelson: In terms of IT?

Mr Simon Clarke: In terms of IT specifically.

Lyndon Nelson: A few. There are some enforcement cases going through.

Q305 **Mr Simon Clarke:** It would be helpful to get examples of the sorts of the cases where this has happened and the sanctions that have been applied.

Lyndon Nelson: Would it be acceptable if we write? I am aware that certain cases are going through and where they are. I can assure you that it bites.

Q306 **Mr Simon Clarke:** From the point of view of your average constituent, they want to know if you are not delivering on what is really at the heart of the banking sector.

Lyndon Nelson: Yes, it is a core responsibility.

David Bailey: One point I was going to make from my own perspective is that having the regime definitely has more teeth than not having the regime. We do not have it in one part of our supervisory architecture, which is on financial market infrastructure. That is precisely why the FPC recently recommended that it be extended to cover those firms.

Q307 **Mr Simon Clarke:** Final question from me. Would there be merit in having a sector map of critical providers? Is there such a thing? As the regulators, do you collectively have a clear understanding of the pinch points and key providers? Is that architecture known to you, or is it deemed that putting that to paper would pose some kind of systemic risk?

Lyndon Nelson: Certainly, we are very worried about the latter case. It is about the degree of granularity. Of course, we know where the major nodes in that network are. It is about keeping that up to date and how detailed we have become.

Q308 **Mr Simon Clarke:** That is primarily your responsibility, is it?

Lyndon Nelson: Yes. We are very nervous about having a map, because it would be wonderful for people who want to cause us harm.

Mr Simon Clarke: It certainly would.

Lyndon Nelson: As Mr Mann highlighted, it would be the one piece of documentation they would want.

Q309 **Mr Simon Clarke:** We can rest confident sitting here today.

Lyndon Nelson: We have the ability to pull that map together.

Chair: I thank you very much for your attendance. It has been a very interesting session. Are you up for volunteering to come back? Obviously, the Committee has the ability to summon you anyway, but it is all the better when people volunteer. You have promised two notes—one in relation to Rushanara, and one in relation to Simon—and we really would be pleased to receive them. Looking around at our hardworking staff and everyone else, I wish people who are taking holidays a very relaxing time. You might come across me if you are camping in the Lake district, but I am sure that most of you will manage to get to more exotic places. It will be a well-deserved break for our staff, our witnesses and the general public. Thank you very much.