Inside FCA Podcast: What does cyber resilience and security mean for firms?

OI: Hello and welcome to the Inside FCA podcast. I'm Ozge Ibrahim and today I'll be discussing cyber resilience with the FCA's security expert, Robin Jones, to talk about what firms can do to protect themselves from cyber threats and attacks. Welcome, Robin.

RJ Hi Ozge.

OI The last decade has seen more parts of the financial system and delivery services move online. What does that mean for us as customers, and for the FCA?

RJ So, as customers, what that's really brought to us is a huge amount of increase in the access to the financial services. You said it's been over the past 10 years, [but it's] probably been the past 20 years that we've now been able to get to what we want, get to our information, move our money around a lot more quickly. At the same time, I think we've come to expect a lot more reliable service. I expect most people want to be able to move money around at any time of day or night, so it's a 24/7 service that we want. Now we want speed, access and we want reliability, and we've really reached those expectations very quickly.

On the flip side of that, of course, those expectations can't always be met and we'll talk a bit more about that later on, but I think that really means that organisations have to be careful when they do create these great services, that they're managing their communications and how customers experience them when they don't work well.

From a regulator's point of view, we need to keep thinking about what's changing, how do we keep up with this? Technology does move very quickly and organisations start to try and use it regularly, so we need to try and keep up with that. As we do that, we need to think about the flip side. So, technology brings all those wonderful opportunities but what about the risks, what about the threats? Who's looking to exploit that new technology and, actually, once it's been put into organisations, how the firms that we regulate maintain it and keep it up to date.

OI Why is it important for firms to think about this and what exactly do they need to do?

RJ We talked a lot about technology bringing fantastic innovation and all the positives that come with that, as you've highlighted. The risk is that, whilst everyone's busily building new and exciting solutions for customers and for their own organisations, they're not thinking about how things might go wrong when they're doing that building. So they're, in effect, building in the potential for future harm - they're building the potential for something to go wrong and then not knowing how to recover from that.

In a world where technology's changing fast, but it can go wrong, you're really talking about people's data and people's money. Those are the two things that people want access to - or potentially criminals are looking to gain access to - and, of course, that leads to harm and that means people haven't got access to their money when they need it, they can't move that money around or potentially their data is lost, and data loss, whilst in and of itself may not lead to harm, it will no doubt contribute to potential fraud and different cyber-crime that might follow that.

It's really important that, when organisations are thinking about a new technology, or even the existing technology they already have, that they are building in the sense of 'how can we be resilient upfront', rather than thinking about it as an afterthought.

OI And are those some of the vulnerabilities we have right now that might have been different to before?

RJ The more technology develops, I think the more complex it becomes. We often think of technology as actually making things more simple. I'm often sure that this might be the experience from a customer point of view, but underneath, there's a lot of very complicated technology that's working to make things appear simple to customers. Because we build complexity in, it does mean things can go more wrong and it means they're more vulnerable to attackers.

So, complexity is one area where I do think cyber criminals will always look to exploit, but I think the other side of this, and the really important side of this, is people. People design technology, they build it, they test it and they use it - and then there are other people on the other side of that trying to exploit it and find gaps in it. You, and anyone in technology, can build an incredibly secure system, but if people are using it, they can be tricked, they can be fooled into giving up their information and, realistically, that's not going away. If anything, that will get progressively worse over time. In effect, what we've done by having more technology out there that allows people to access financial services, is we've given criminals more direct routes to access customers.

OI But what can firms do now to stop some of this from happening?

RJ So, one of the phrases that gets used in the technology world, which we have to be a little bit careful about, is what's called 'designing things that are secure upfront' or 'secure by design'. It's a nice phrase for technology firms to use, but really what we're talking about there is 'do you think about security when you start building something from day one?' Too often, it comes along afterwards where you discover someone's built an amazing thing that's going to do something brilliant for their company and for their customers, and then someone says, 'but what about security after that?' And actually, you want that forethought to really consider 'how do I build security in upfront?'

OI Robin, can you talk us through some of the main implications of these attacks on firms and their customers?

RJ Criminals will often be looking for money or data, and that can have a very immediate or, potentially, quite a long-lasting effect on customers. I think it also undermines trust in the industry and trust in those individual organisations but, potentially more widely, where customers begin to think about whether these are organisations they want to use.

We do a lot at the FCA to understand what's going on in the sector. Some of that is information that firms we regulate report to us as one useful source of information, [but] it's certainly not the only one. We recently published our sector views - looking ahead to the kinds of things we think are going on in the different sectors we regulate. In there, we said there's been a 7% increase in technology outages in the year 2018 to 2019. The interesting thing about that, of course, is that might not be because there's been more cyber-attacks and more technology outages directly, it might be that organisations are getting better at telling us about them. So, we have to be slightly careful with the data.

Nevertheless, we do see [that] one of the areas where firms are still weak is in cyber security. We also see firms are actually making a lot of changes to their systems a lot of the time, and those changes will, on occasion, not work effectively and, when those things do happen, we don't see industry knowing how to effectively respond to keep customers updated, keep them informed and manage the situation effectively.

I don’t think we should get this too wrong though. There’s a lot of organisations out there that we regulate that are doing a lot to try and prevent cyber-attacks. There’s a lot of investment going on out there, but we just have to be realistic and accept the fact that they will work, they will be successful at some point. So, we’re asking organisations to think about how they would respond when that does happen.

OI And what are some of the things that firms are doing to prevent attacks and associated disruption?

RJ So, one of the key things that we’re asking organisations to think about now actually is do they know their business? So, do they know how their business works, what services they provide to their customers and how does the technology data people process all stack up to support that? Actually, that’s a real beginning point. So, we’re not having a conversation that says, ‘do you understand your technology in detail?’, it’s a much broader one about understanding the business.

If they then understand how their business works, it should be easier to understand where it needs to be resilient, so, what are the most important aspects of the business that need to stay resilient and then think about how they would respond when something does go wrong. So, we are trying to shift the conversation away from stopping everything from going wrong to, it will go wrong and, if it does, what are you going to do? How do you continue to provide that service? Maybe in a different way to the way you do now - or in a manual way if you have to – and how do you effectively communicate after that?

Your systems are only as secure as the people that use them, whether that be your internal people or your customers. When organisations make change that is where things tend to go wrong, so, how would you manage that, how will you make sure the change is effective? Really, we’re talking about the basics of cyber hygiene, if you want to call it that, and operational resilience.

OI Can you explain what cyber hygiene means?

RJ Yes, it’s an overused phrase and I’ve just used it again. This is really about getting the basics right. Cyber sounds very complicated, it’s almost, in some ways, designed to sound threatening I guess. But actually, this is who accesses your system and your data right now. How will you know if that changes, how do you know if different people join your organisation, if they leave or if a new third-party supplier is brought onboard, how do you know that they've got the right access to the right information? And, then, how do you keep your technology up to date?

Many people have phones and computers that say, 'are you ready to upgrade?' and you click on the 'yes, I'm ready to upgrade' button. You'd be surprised how much of that doesn't happen from a technology point of view, because organisations we regulate find it very hard to say, 'yes, I'm just going to upgrade' because the complex systems they've built just don't lend themselves to an easy upgrade.

It gets called patching in the technology world but, realistically, it's about staying up to date with your systems and your software and keeping it current, and that's not as easy as it sounds. So, we're not trying to make cyber hygiene complicated, it should be pretty simple. I think it is also worth flagging that we've published a few infographics as the FCA on good cyber security, getting the basics of what we call 'network security' right. Those are already available on the FCA website if you search for 'cyber resilience'. We also published an insights document, which is a document that's actually insights from industry about how to be more cyber resilient, so it's advice from industry to industry, it's not the FCA saying you should do these things, it's shared experience from conversations we've had with firms and we think that's incredibly powerful.

And the other place to always look for advice on cyber security is the National Cyber Security Centre, NCSC. They have a huge amount of advice, it's not financial services-specific but it doesn't need to be, and it sets out some really key information that everyone should be looking at.

OI Robin, what role does good governance and leadership have when it comes to tackling cyber threats?

RJ I think governance and good leadership are absolutely essential when it comes to identifying, tackling and responding to cyber threats. At the end of the day, leadership sets the tone in an organisation and if they're not seen to be taking this seriously, it's unlikely that everyone else will as well. There is most definitely a top down approach to this, I think, which is about showing to other people that your senior people are taking cyber security and resilience seriously.

Saying that, there's also work that can be done with your people on the ground, so we shouldn't always assume this is a top-down approach.Often when we talk about this we say, 'well, our people clicked on the wrong email, it's their fault, why did they click on the phishing email and let a virus in or some malware in?' Actually, that's not about the individual, it's about the culture of the organisation and whether you've actually helped those people identify those emails first, rather than just automatically assuming that you should blame them. Those individuals are an incredibly important part of spotting suspicious emails, which is often the way into organisations, especially the smaller ones that we see, and you don't want them to just be blamed for having got something wrong if you didn't set up a culture and an approach and a way of thinking on the ground that helps spot these things before they happen.

OI And is it possible to create a good security culture and what does it look like?

RJ I think it is. There's no perfect security culture out there. So, I've just talked about the fact that we shouldn't really be looking to blame staff if they click on the wrong thing or open the wrong attachment - and how important they are to maintain resilience - but there are other ways you can help build that culture. So, you can test your staff, you can send them fake phishing emails, which is often quite revealing as to who's a bit too relaxed about opening the wrong things, and that gives you the opportunity to educate and support them, rather than point the finger.

The other way you can do this is there'll be a huge amount of personal information available online to you about your staff. And, actually, if that information is available to you, it's available to criminals, and you might rapidly discover that some of the people that look after your technology have managed to put a lot of their personal and work life online. That's a really useful route as a criminal to then work out how to manipulate that individual to give up certain information, or click on the wrong email – again, because it's been made to look incredibly convincing using all that external information.

So, you can find other ways of saying to people, think carefully about how you would like to protect yourself and your own personal data. It's not just about protecting the company they work for - but we all worry about that - so why aren't we applying the same things that we worry about to the way and the place we work in?

OI And what can smaller firms with, you know, possibly less resources do to tackle such threats?

RJ So, I think for smaller firms we need to keep making sure that this message is simple. It does need to be about the cyber basics. I've said before, there's a lot of really good advice out there and a lot of the National Cyber Security Centre's advice does focus on smaller organisations - there's lots of good practice that they share on there. Most small organisations will have one or two systems, they'll have their email system and they may be storing some information elsewhere. It means they've got a relatively small place to focus on being secure but also recognise that's where the vulnerabilities lie. A lot of the cases we see with smaller firms involve email and those emails being intercepted or redirected by criminals, so, if that's the main source of how you do your business, that's the place to focus your efforts on being resilient.

OI The Bank of England, the Prudential Regulation Authority or the PRA and the FCA have recently published consultation papers on new requirements to strengthen operational resilience in the financial services sector, and one of the areas of focus is greater resilience of the cloud and other technologies. Can you explain why this is important, Robin, and the outcome of the consultation and how this might impact the future of regulation?

RJ The FCA, along with the other regulators you identified, started a consultation on this at the beginning of December last year. It starts from a premise that I've mentioned a couple of times – we don't expect that firms will be able to provide a service all the time, constantly 100%. I think the better way of saying that is we know things will go wrong, and we want firms that we regulate to be prepared for when that happens. We want them to then think about the harm that could be caused if their customers can't access their services, if they lose their data and so on.

So, we're trying to get a message out there which says we accept that failure can occur but we would rather that organisations understood where that's most likely to happen and prepare for it.

So, the consultation paper sets out some key concepts. We ask organisations to understand their business, as I've talked about before, we call that identifying their business services, so what services do they provide to their customers - and those customers could be retail customers but they could also be wholesale market participants as well, they don't have to be the retail consumers. If they understand how their business works, the next question is what of those different services are the most important ones? So, some services they provide are incredibly important both to the organisation but also to their customers, and we ask them that they think about that prioritisation whilst thinking about what the regulators care about. So, if it's the Bank of England, financial stability; if it's the Prudential Regulation Authority, the safety and soundness of those organisations; if it's the FCA, then it's really going to be about the harm to consumers and the markets.

And so, prioritising what they do and how important it is - based on what we think as much as how if something went wrong how that would affect their organisation - should mean you get to a relatively short list of 'what do we care about if it goes wrong?'

From there, we then say to those organisations, 'okay, how resilient are those services we've just talked about, are they as resilient as you would like them to be?' so 'what's your tolerance for disruption?' And really, what we expect to see is that, when firms then start to test that and see how resilient that are, they will find gaps. I'd love it if every organisation we regulate said, 'no, no, it's fine, all the services we provide are incredibly resilient and we haven't got more to do'. That's not our experience so far, and you can see that in a lot of the more public examples of things going wrong.

So really, the challenge to organisations is, 'you're not as resilient as you would like to be or as we would like you to be, how are you going to get there?' And that probably is an investment and a prioritisation conversation that those firms need to have ultimately at a board level. It's really a senior management and board level discussion.

We've talked a lot about cyber in this discussion. Cyber threats, cyber resilience is part of that operational resilience agenda, so it's not separate, it's not different, it is a different cause of disruption because it's somebody trying to do something intentional, they're trying to disrupt and steal but, at the end of the day, the consequences are the same for customers whether it be a cyber-attack or a change that went wrong.

That this isn't something organisations can do overnight, it's going to take time but that's the challenge we pose.

The concept of operational resilience is challenging firms to think about the outcome of resilience, how do they become more resilient and therefore reduce that harm? We, as the regulators, can't tell industry how they should run their business, we don't know what those services are that they have, we don't know what tolerance they should set for disruption, but what we are saying is resilience is likely to be a core part of a business model for an organisation in this increasingly digital age. So, how do you achieve that resilient outcome? That is a shift in the way we would talk to industries, a different way of thinking about regulation because it's saying, 'we've given you some parameters, some challenges, now you go away, think about them and come back and tell us how you intend to respond to be increasingly resilient'.

OI And what responsibility do we as individuals hold, if any, to contributing to the resilience of the wider financial system?

RJ We all have an individual responsibility to ourselves to stay resilient and understand where the threats might come from, and how we protect our own data and our own systems. So, I think if we can apply that kind of discipline and effort that we put in to doing that for ourselves into wherever we work, we're already contributing to the resilience of the system. If we're not clicking on those emails, if we're being thoughtful about what kind of information we have on social media - that supports people to exploit that – and if we're really calling out areas where we start to get worried, and if we see things that don't work properly, that can be incredibly powerful.

So, I think that works at an individual level and it contributes to that culture of cyber resilience.

OI So, looking ahead, is it more of the same or will there be threats from completely different areas or different parts of the world, for example?

RJ We will always see the threat that relates to people. People are always going to be that vulnerability and they will always be exploited and criminals will look for that every time. One area where I think we might see more of that is, we spend a lot of time making sure that we're secure when we use our laptops and our computers at work and the big systems that industry uses to provide financial services, we don't spend as much time thinking about the security of our mobile phones. Those are the things that are in our pockets all the time, they hold a huge amount of very sensitive information and I worry that we perhaps think of the corporate side of security but, actually, a lot of us are probably using those phones just as much for corporate activity now as they were before.

So, I think maybe we need to start thinking that we're incredibly mobile now as a workforce and, actually, are we protecting that aspect of it?

If we look a bit further ahead, there's a real challenge down the line with what's described as 'quantum computing'. There's many different ways to describe that, which would take a very long time and more intelligent people than me to describe, but, ultimately, quantum computing will massively speed up computing power and, when it does that, it will, in effect, break a lot of the security that we have around our computers, our laptops and our mobile phones overnight. Once somebody has quantum computing power, they can break in because they'll have the power to unencrypt or decrypt a lot of the security layers that we have in our systems.

Now, that is something that people are working on to try and build alternatives that would mean that when quantum computing comes along, there's already a quantum computing answer to that question. A lot of people spend their time focusing on the benefits of quantum, and there are huge benefits in how we would speed up decisions and processing of data, don't get me wrong, but the flip side is it creates a significant security risk.

So, that's one we always look ahead to. It could be in 2 years' time, it could be in 10 years, it could be in 20 years' time, I'll probably be in the middle of that debate somewhere. When it happens, we're going to need to be ready and I'm not sure how ready we are.

OI Well, that gives us a lot to think about for the future then. Thanks for your time today, Robin, and your insights into this important and fast-moving space. I'm Ozge Ibrahim, join us again soon for the next Inside FCA Podcast.