

Event overview: Is Your Workplace Future Ready? - October 8 (11am-12pm)

We held a debate focusing on three big questions, which face Financial Services and Insurance organisations:

- **Trust** – Creating a culture of trust, loyalty, and connection with all stakeholders through this uncertain time and beyond requires leadership, resilience, and decisive actions. What changes do you need to make: foster greater trust with your shareholders, employees, suppliers, partners, and customers? At a tactical level, how do you secure devices, safeguard networks, and protect financial data when staff are moving between the office and remote working? How do you create greater operational and cyber resilience in response to an increase in COVID-19 related cybercrime?
- **Productivity** – Reimagining your business model to focus on productivity and growth that leverages technology. How does this current pandemic present an opportunity for you to reshape your company to focus on new workforce models such as hybrid/remote working, full remote working, or partial return to workplaces?
- **Safety** – Creating safe and secure workplaces. What changes need to happen to ensure the ongoing health and wellbeing of staff and customers as they return to workplaces? How do we reconfigure workspaces for the long term, whilst adhering to social distancing protocols, deploying testing track & trace systems, and using data insights to help create safe spaces?

Speakers from Atos and Dell Technologies

 <p>David Haley SVP, Global Head of Business Transformation Services & Head of FSI Northern Europe – Atos</p>	 <p>Margarete McGrath Chief Digital Officer – Dell Technologies</p>	 <p>Glenn Mallon Senior Director, UKI Financial Services and Insurance – Dell Technologies</p>
---	---	--

Audience

Financial Services and Insurance organisations – globally: C-Level attendees

Roundtable transcription

Speaker	Conversation
David	<p>Welcome.</p> <p>I'm David Haley, SVP, Global Head of Business Transformation Services, FS&I at Atos, and I'm delighted to be joined today, both in beautiful locations according to their backgrounds, by Margarete McGrath from Dell Technologies, who is the Chief Digital Officer, and Glenn Mallon who is the Senior Director for UKI, Financial Services and Insurance for Dell Technologies.</p> <p>We're also joined today, of course, by some extremely esteemed customers of ours and we're very excited to have colleagues here, and going down the list of attendees and looking at the blogs and looking at who we have with us today, we've absolutely aced out on the round table in terms of relevance for what we're going to be talking about today. Myself and the panel were getting rather excited about the discussion before you all joined. There is the opportunity to be able to, I guess, share best practice, share where we're at. These times are weird and changing here in the UK, which is about to go into another step of restrictions, we understand, at the beginning of next week, which we're not quite sure about. So the timing of this event, and indeed, these topics, are so important.</p> <p>Ourselves and Dell Technologies enjoy an extremely good partnership, and we're market leaders, particularly in the power of which is now being used to support customers around the world as they return to work and return to the workplace, I should say, because, of course, all of the things we'll be talking about today, is the fact that people did come to need to work, but not necessarily in the traditional methods which we're used to. So we're looking forward today to hearing about insights, some of the thoughts, some of the experiences, that you are seeing. We'll certainly hear from our colleagues in Dell Technologies about what they're working on and how they're helping us and our colleagues to be able to support the return to the work environment, as well.</p> <p>And I guess, just thinking about this whole movement back into the workplace, if indeed organisations did leave the workplace ... I know in the case of my staff, we simply couldn't remove ourselves from the workplace. One of our customers that we manage, we are actively engaged into the live bank, into the core banking engine, so the ability for those colleagues to be able to work from home was impossible, given that we are connected to the bank. Having said that, we were able to look at some of the business operations and decide who could work from home and who could not, and fortunately, or unfortunately, whichever way you look at it, stay in the work environment.</p>

So, I think the big question that's on everybody's mind at the moment is - are the traditional working environments really ready for, I guess, the 'new normal'? Which is a term that we hear a lot. And how do we ensure safety? How do we ensure that that's intelligent? How do we ensure that the workplace is able to deal with the demands now upon us, as a result of the new restrictions?

And also, I guess, for me, how do we support our colleagues? How do we make sure that they feel comfortable, that they feel safe, that they feel secure? Because they are essential workers. One of the things that the UK government unilaterally did do, at the time of COVID-19, was agree that everybody in financial services was an essential key worker. And that, in itself, caused some consternation and some confusion across the environments. But what I think, in the main, we accept and welcome that, because we know that in financial services and the insurance world, it has to keep operating, particularly in this new environment.

Gartner have shared a piece that highlights, in order to successfully reset the merge from the crisis, it's critical that financial services align their next steps with business executive leadership strategy. So what should this strategy look like?

So, I think, for me, it's one of the things I'm really keen to understand.

We are going to be exploring three particular areas today.

One is building customer and employee trust, one is increasing employee productivity, and the other one is ensuring the safety of everyone, which, of course I'm sure is paramount to everybody's objectives. So, thinking now then about how two and a half times more people are working from home than there was, certainly 60% of my workforce moved from working in an office to home. And of course, subsequently, there has been an increase in phishing attacks and breach of security attempts on the infrastructure, more than three and a half times the growth, particularly in areas that we've seen ourselves. Enabling trust, but whilst also safeguarding the data is a major challenge for, I guess, all financial services organisations. Business needs to be looking at ways to build that staff confidence by safeguarding their devices, networks, and data whilst also building, of course, most importantly, consumer confidence that their data will be safe and will be managed in the right way.

Margarete, let's come to you, if I may. So what changes do you think financial services and insurance companies need to be making to build and maintain the trust, not only with staff and customers, but also, I guess, with shareholders and suppliers?

Margarete

Brilliant segue into the conversation, David, so thank you for that and great to be on this discussion panel. I think, from the conversations we're having with a lot of our client base and customer base in financial services and insurance at the moment, it has caused a significant shift around remote working and how they adapt quickly to remote working, and has exposed a number of vulnerabilities and gaps around data protection, around the right security, their private, and personal networks. So, there's a lot to consider around the cyber element of this. And now that we're seeing some movement, and I know it looks like it's inevitable that we may see further lockdown, I do think the physical aspect of even branches and bank branches is coming into play around security there.

There's a broader debate happening around privacy and safety, and how much data we want to release in terms of what do we want to sacrifice in terms of getting our own safety right. But I think there's two realms of this. There's the remote working element and there's the physical side of it as well, and trust needs to be built in both, with consumers and employees. So, we're seeing organisations scrambling to put in the right cybersecurity measures, the right risk protocols. And for most of them right now, they've done it very quickly, but they haven't got it done in a sustainable way. I think they're going to put in longer-term plans to really try and lock down workplaces and datasets and to make sure that remote working is set up for the future. I think that will continue. I don't think that we've got that right. I think there're lots of organisations that are scrambling around trying to figure out, just from even a private networking perspective, how do we get that right?

We are seeing significant rises over the last few weeks of phishing attacks and ransomware attacks, but I think, even if ... I went into the bank branch, I was telling this to Glenn, our colleague, the other day. And I went into a bank branch recently, my local bank, and there were so many delays in the bank because they were trying to make sure the right physical distancing was in place, where you don't have one counter up and that sort of thing. And there's always a little bit of a trade-off here around productivity and safety. If they put in the right safety measures, it will definitely slow down productivity within bank branches.

I think there's a lot to grapple with here. We are definitely seeing, on the remote working side, we have not got that right from a trust point of view. Certainly, our plan and what we're doing at the moment, is working in partnership with a lot of the large insurers and the banks around kind of getting security right, but I think the physical elements of going back into bank branches or credit union branches is equally as important. And that security element, safety measures - we still haven't got that right.

	<p>And I think the government legislation is kind of chopping and changing, so it's not easy, but I think one thing that is coming through is having a clear plan and writing and iterating that plan all the way through. But we are seeing with cybersecurity, huge vulnerabilities right now and great exposure. And so it's got to be addressed very promptly. So agility is needed in all of this.</p>
David	<p>Yeah. That's really good. And it's interesting to talk about the bank branch and the productivity and, I guess, the expectation of when you go into a bank branch, as well. What are we expecting these days? What is that productivity and how much tolerance are we allowing, I guess, in this new world in the way that, previously, we would have been sort of touching and expecting to get to the front of the cubicle quicker? but actually now, there's a little bit more tolerance there. So it's that give with productivity versus the need to have that security in that place.</p> <p>I guess, just going out to ... We said it's going to be a conversation. We said it's going to be interactive and collaborative. So can I reach out to some of our colleagues that have joined us from other organisations? 'Customer' what are your thoughts?</p> <p>Just thinking there about what Margarete has said. What are you seeing in terms of ... obviously not the bank branch situation, but what are you seeing in terms of that trade-off between productivity and safety and security in Insurance?</p>
Customer	<p>I'm not sure how much thought I've given the physical environment, to be fair, given that the vast majority of everybody is working remotely.</p>
David	<p>Is that your situation? Have you got a lot of people working remotely?</p>
Customer	<p>Yeah. There're basically no people that are in the offices right now. For a mix of reasons. They're not necessarily in the appropriate environment, from a wellbeing perspective or a security perspective. They can't be sitting out there in the open talking about customer details and whatnot, if they've got other family members around.</p> <p>And then the other side is just from a wellbeing perspective. Those people that are in the offices right now, and the office itself, does not represent what it used to be, if you know what I mean. People had, certainly at the start of this, had this ... well, not necessarily at the start, but once we kind of moved from what we called a red phase to an amber phase, it started to slowly free up and enable people to go into the office. I think peoples' ideas of what the office was going to be like were fundamentally different from the reality. You don't necessarily get the same buzz in there because everybody's distanced. You've got the one-way things here. It's a pain to navigate, if you like.</p> <p>But from a safety perspective, all that stuff is in place and we're pretty militant, from that perspective, including with our executive committee because they like to be in the office. But, yeah, from a customer</p>

	<p>perspective, I guess we're talking less about a physical environment, the working environment, and we're talking about our ability to meet their needs and give them the confidence that their data is protected, that kind of stuff, because, I don't know ... Other than the challenges with the risk that is presented through the actual physical environment when you are at home, like I alluded to around what you're talking about in terms of sensitive details, anything like that, firstly identifiable stuff.</p> <p>The technology, itself, has not fundamentally changed in terms of the security, the AV, the VPN side of it, the firewalls, and stuff.</p>
Margarete	<p>Yeah. I guess, 'Customer,' just for you, do you expect that we'll actually sustain a more remote working kind of plan over the next while? Will you invest differently now in that technology or you figure you guys have got it right and it's up and running and it's working well?</p>
Customer	<p>I think the reality is, regardless of where someone is located, we need to ...</p> <p>I think that the nature of the security, the need to protect data endpoints, all that stuff, move to zero trust, I think to an extent transcends geography and the fact that you're always going to have kind of motivated threats out there in the world. I'd be interested in someone else's views, maybe someone that's more kind of specialist in the security sense. What's fundamentally now started to present itself, in terms of a threat, or what's being exposed as a vulnerability that links to where someone is working?</p>
Glenn	<p>I see what you're saying, 'Customer'. I think the threats are the same because they're always evolving. Right? Because if anything, it's just gone into hyper-speed a little bit.</p>
'Customer'	<p>Yeah.</p>
Glenn	<p>Trying to take advantage of the opportunity. But I think the real challenge here is the escalating complexity that people aren't ready for. So you have a stack of only so many and then you have this load that's hitting you. And all of a sudden, you've got to restack up for it or add more or reposition people within your environment. And then there's a whole lack of qualified individuals in that area, anyways, which was a market challenge prior to this. Right? I really believe that there's really no new thing that's coming up. There's just a whole load of different stuff that's kind of the same, trying to take out your access. That seems to be the big one still, and it always will be.</p>
'Customer'	<p>Yeah.</p>

David	<p>Glenn, given you're in the chair, trust is hard to win, as you know, but I guess easy to lose. And given what we're just talking about here, and 'Customer' makes some very valid points there about security, et cetera, what do you think we should be doing to regain that trust?</p>
Glenn	<p>I think we can all agree that it's just a matter of <i>when</i> you get hit by something rather than <i>if</i> you're going to get hit by something. And it's been like that for a while now. I think trying to defend the attacks is always going to be a focus area, which it should be. How do you recover? That's the real key here and that's where the trust piece comes in, because you expect your customers to believe that you are constantly trying to stay ahead of the game because you're a big corporation, they think you should be doing that. But how do you react when you get hit? And the newspapers love to go crazy on this. They love to monster that and the consumer really listens to that. They don't understand the details.</p> <p>So, we work very well with providing wealth services, which takes data that's unchangeable, it can't be changed, and we give you a position where you can recover your organisation very quickly. And that, for me, if a company gets hit, if you look at the SEC, all wealth management companies in the US now have to have evolved to some sort of play. The first thing a consumer wants is, "Okay, you've been hit. Where's my money?" They don't care about you, as a company. They want to know where their money is and they want to see it and they want access to it. So if you have the speed, I think the trust and speed are really tied together of how quickly can you get up, and that will maintain trust. You'll have some people that will be like, "You're done. I'm out." That's just normal, but it's trying to attack the majority. Right? I think, personally, how you recover is a real focal point with the trust piece.</p>
David	<p>That's actually interesting, isn't it? Because, I guess, as you say it, it's the 'when', not 'if' mentality. I think we all need to have that. And I think 'Customer' spoke about that, as well, but also that's an interesting take on, actually, I'm more interested in 'me'. How does that affect 'me' at the moment, rather than how did that affect your organisation? And I guess, thinking about home working and thinking about, as 'Customer' has just alluded to there, and certainly from my experience, 60% of my workforce continue to remain working from home and delivering important, critical services. But the attacks on the home working environment have massively escalated over the lockdown period. I mean, going from something like 12% attacks on home working to something like 65% attacks, potential attacks on home working over that period of time.</p> <p>So getting the security is clearly a massive part of trust, which has just been talked about. Margarete, how do you secure devices, safeguard your networks, and protect the financial data, that, when your people are moving around between office, home working, especially when we've</p>

	<p>seen the increase in COVID-19 and the cyberattacks that you've just been talking about?</p>
<p>Margarete</p>	<p>I think a lot of it comes down to awareness. And I think, Glenn, first on the element of recovery and what do you do when you're attacked, I do think ... and I spoke to one major bank yesterday and they have ramped up significantly coaching, training, great awareness and they're actually bringing in new technology, like biometric security as well, for the trainers to continue working remotely. So they're going to stack up security over the next while. And I do think the awareness and the education on this one is a one-off, we all need to do it, and as leaders, drive that through for remote working staff because I don't think any of us expected this to go on for so long. I think we're going to see a sustained amount of the workforce remain either working in a hybrid model or working at home.</p> <p>And so I think it's putting in greater safeguards, particularly around virtual private networks, particularly on data protection. I think those are key. I also think we have a significant amount of IoT devices and edge devices in our home. And I look around the room that I'm in, as well, and there's an Amazon Alexa, there's a Google Next. And so that could catch anybody off guard. Understanding where the exposure points are, not that we all want to be cybersecurity experts, but I do think the vulnerability, working remotely, it has risen and it's safe. I do think, actually, education and awareness is going to play a critical role and that needs to come from the top down for a lot of these financial institutions and insurance companies.</p> <p>And some of them have already started that program. One of the banks yesterday was sharing that kind of detail with us, saying they're exploring new security technologies around biometrics to bring in greater safeguards. And they've kind of given guidelines now to where staff should and should not work. So Starbucks, Costa Coffee, those places are saying, "Please do not go there while you're working. Take the time out, but don't bring your endpoint devices." There's a lot to cover off here and I think they're baby steps, but I think we've got to get the education and awareness right and make people aware of the increase in vulnerabilities like that.</p>
<p>David</p>	<p>Yeah, it's a weird ... I mean, we were talking before the call opened up and we were talking about, if nothing else, COVID-19 has forced the digital issue. It's forced the fact that we are fundamentally changing the way that we operate, the way that we work, the way that we have built our expectations. And interestingly, you're talking there about baby steps in certain areas, but actually on the back of a quantum leap that the whole industry has had to take in the face of adversity that none of us could've expected. I wonder, is there anybody else from any of our customers and esteemed colleagues around the virtual table, anybody else got any other experiences that they wish to share in terms of what their learning has been to this particular time around security, around the need to create</p>

	<p>that safety, but also security, as well? Anybody wish to share any of their experiences that they've seen or, indeed, challenge some of the thinking that's got into how security has been brought in for your environments?</p>
<p>Margarete</p>	<p>I guess it will be good to turn on around. And it's good to hear your perspective, David, around if you're seeing, from your customer base, a rise in the importance of security and risk management, because I think every ... So, from our side, from the Dell Technology side, we are seeing a much more heightened approach of assessing risk right across the enterprise and across the organisation. It'd be great to get your insights on that one.</p>
<p>David</p>	<p>Well, risk is a very interesting area. So if I think about one of the major banks that we look after, for example, they have had a 100% risk averse mentality in place for many, many, many, many years, over a hundred years, but they need to grow and they need to continue to be able to operate. And actually, what we've seen is, I guess, a reliance to work with partners, who in the case of this bank is us, to say, "Well, look, you manage our infrastructure, you manage our environment, you manage our processes, you manage the way that we operate this bank. What do you think?"</p> <p>And that 100% risk aversion has actually led to ... I wouldn't say a relaxation in risk, but I think there's a different risk appetite. I think sending people to work from home was always here, but they could take photographs on their smartphones and share that information. But actually, and I think 'Customer' made the point, you've got colleagues who've had to go and work from home, but operate in exactly the same environment in terms of mentality, in terms of the risk, in terms of the operational excellence that we expect to deliver for their core organisation and in exactly the same way as they did when they were in the office.</p> <p>So I think it's been a really interesting ... I think there's a lot to learn from what we've just gone through. I think the big challenge we've got is we've learned a hell of a lot in a very, very short space of time. We've got to capitalise on that. We've got to capture that learning. We've got to refine that and then I think we almost, not rewrite the risk policies, but I think we almost need to adapt the risk policies and the risk appetites that have come out from this period of time while it's looking at the net promote scores, while it's looking at the service that our customers and our customers' customers expect and also, I guess, the risk appetite of customers. It doesn't seem like long ago that you wouldn't trade online in case somebody stole your credit card information when you were shopping online. And yet, probably the best job to have in the United Kingdom at the moment is a Sainsbury's delivery driver because</p>

	<p>everyone's shopping online because we just don't even think twice about it. We just assume that there's going to be a level of security in there now.</p> <p>So, I think there's been a change in mentality, from a customer perspective. I think there's been a radical rethink, from a client's perspective, and from an organisation's perspective. I think what we have to do now is marry those two together so that, when we referred to the 'new normal' before, we need to marry that together, assuming that the technology and partnerships, such as Dell Technologies and the work that we do for our customers, this is the kind of stuff we're all worrying about all of the time. This is what we're ensuring is in place so that, actually, the organisations can focus on customer service, can focus on productivity, can focus on the safety and security of the employee in the workplace, wherever that is, but also the agility that they now have as a result of digital capabilities - we have to work from home and in exactly the same way it could be if you were working from an office environment.</p> <p>I think that's the big change that we're seeing and almost that sort of allowance now from the core bank or the core financial organisation to really leverage the strengths and the capabilities of the partnerships that they have around them to say, "Well, what do you think we should be doing now?" rather than, "We've got all of the answers and you're there just to implement what it is that we need to do." So, a strategy rethink, and a risk rethink, I think, is definitely on the cards and we're servicing that.</p>
Glenn	<p>Look, you say that was an operational level, right? Everything was based on personas. You are a corridor warrior or you're a salesperson on the road and your whole security profile was always tied to that. So you're somebody that's always in the office, while we can just have basic, standard stuff on your desktop, which seems to be a thing of the past with the declining market share in that for everyone, and everyone's going to laptops. Now, it's actually personas that have changed completely. They should be at, what's your role? What's your role in the organisation? Are you HR? Are you sales? Are you operational? Are you IT operations? Are you back office? Are you front office? Whatever it is. And if you look at changing it, definitely make everyone now a mobile worker, because, number one, the productivity has been proven, inside and out. And for the security piece, you add an extra layer. You add a unified comms piece, which will give you the same experience, same secure access to any application needs, regardless of the device used.</p> <p>I know Dell Technologies isn't exactly a financial customer, but we are a 165 thousand-people organisation. So we're the same scale with the same challenges. We approved our VPN so more people could get onto it. And honestly, that was something that everyone's had to do. So you said earlier, David, that it took you guys a week to get everyone up and</p>

	<p>running. We changed the personas and how we actually approached that, immediately. And by the way, Dell Technologies has been in the remote working business for 12 years now. We're vets at this stuff, but we still had to change, as well. But I think, by implementing rollout, we're now going through a massive phase in implementing workspace, what we're calling our connected workplace, which truly allows you to access applications that are, so ...</p> <p>Here's a 'for instance'. You have email. You have to change your password on your laptop, then you have to change it on your tablet, then you have to change it on your phone. Now, through the workspace one that we use, you change it once and it just perforates all over. And so a lot of people can't remember their password because things are made easier, biometrics, et cetera, et cetera. So it's just those little things to keep people productive, keep their trust, keep them feeling confident that the company is really looking out for them, helping them to be productive. I think, if we look at it from those perspectives, security and productivity, it's so tied together, as you were saying. I think change has to happen at every level. That's really what I'm talking about.</p>
David	<p>I guess what you're saying there is, actually, it doesn't really matter whether you're in the office, whether you're in the home environment, or whether you're mobile, or agile and working around. Actually, that sense of ... because we kind of rushed to this new world, didn't we? We rushed to this. I mean, we were talking before, weren't we, about there's been a strategy in place for many, many years to improve the productivity of the workforce, to improve the comfort of the workforce, to allow people to have more flexibility. And yet, after the pandemic hit, we all kind of rushed there. And I'm sure a number of us made shortcuts. I'm sure a number of us had to. As I said before, within six working days, we had to get almost 100% of our contacts on that capability. There was voice recording, and digital recording, and safety and security, et cetera.</p> <p>And what you're talking about now is that agility, but that new service that can be brought in that says it doesn't matter where you are. Actually, you're going to be able to be productive. You're going to be able to be online, safe, and secure. And I guess that's really important, isn't it, to understand how, from an employee's perspective, that's important, but from an organisation's perspective, that's got to be critically important, surely?</p>
Glenn	You need the confidence of your people. Right?
Margarete	Yeah.

Glenn	Everybody.
Margarete	<p>Yeah. And I think, to echo your point, I think it's been quite seamless from a user perspective from our side. That's been the real secret to it, is that it's just been done so seamlessly. And we know our security has been wrapped up considerably. Even in the last week, actually, our Zoom profiles have been tightened, as well. And so for many of us, as users, it's been a fairly seamless journey, but we know that security has been significantly invested in over the last couple of weeks and months because we're preparing for the long haul, right? Even though we've always had remote working, there's been quite a step change in security and kind of risk processes.</p>
David	<p>And I guess, Margarete, from your perspective, you must be constantly evaluating what you need to do to ensure that safe workplace?</p> <p>So, if you could give us some examples of what you're having to go through, just to ensure that you're on top of that.</p>
Margarete	<p>Well, one of the things, there's regular training, but I think as Glenn touched on, the seamless interface of signing at different platforms has been standardised now. It's been upgraded and there's a lot more protection around single sign-on. I think then, for certain data exchanges, it's been tightened. We've rolled out kind of new advancements in terms of private networking security and our endpoint security elements. So that's all been driven down from our security teams, but it's constantly being assessed. So Dell always had that remote working strategy and we were always kind of solid on secure personas per role. Now, everybody's a mobile remote worker. So I guess the security elements of that have just been completely overhauled in that, but it's been done in such a way that, actually, for us as users, it's kind of subtle. We don't really notice it. We know, Glenn and I do, that it's actually been quite significant changes, both from a networking and single sign-on, endpoint security, and that's gone through. And then there're different levels of authentication, as well, for different data that's happened.</p> <p>And that's been replicated with a lot of our customers, as well. So we're rolling out what we did internally to our large customer base and then financial services. So we can kind of share the journey of how it's worked, what are the lessons that have been learned, but it will continue to advance. No doubt that security investment will increase. And actually, one of the feedbacks we're getting from some of our own customer base is just the fragmentation of the investment that they've made over the short period of this pandemic, over the last six months, in an effort to get things right. And now, they're looking to consolidate that. They're going, "Okay, how do we protect the whole enterprise, the whole business?"</p>

	<p>And so some of them are putting in new agile ways of working, agile assessments around risk, and they're spreading the kind of response, not just so that it sits within the security function, but actually it's with every line manager.</p> <p>So quite a shift in leadership and capability, as well, to say anybody that's in the team is responsible for security on that team and driving that out, as well. Glenn, have you any other points you want to add on that from our journey?</p>
<p>Glenn</p>	<p>Yeah. So if you look at returning to site and the safety of that, so we're going through a thorough process at the moment, globally. So in the UK, we just opened up some of our office on October 5th and we've gone through a whole process with the individuals through surveys, as well as confirming with management, does this person need to be in the office? And the whole need to be in the office wasn't down to their role. It was more down to their physical wellbeing. Right? Are they not able to work from home? For a lot of different reasons. We see Zooms. We see some of our younger employees who are just coming from Uni. They're literally sitting, working on a couch, on a table because they're in a flat share and their private broadband is up and down and it's not conducive to working and they're uber insecure about it. So how do we get them into a safe environment?</p> <p>Like everyone, we've gone through the whole protocols in our offices and we've given two metres of spaces. We've identified desks where people are named to desks. And from a digital perspective, we actually ... because our London office in particular, which I run, is more of a hot desk area. So we've got an application coming out where people can digitally sign on and rent the desk out for the day. And that's their desk. No one else can touch it. And if you don't have a desk rented, or, not rented, leased ... rented, leased, same thing I guess, but if you don't have it booked, you do not get in the office. So it's to create that safe environment, right?</p> <p>And the thing that's interesting, if you look at some of the protocols we'll put into the walking in area where you have customers and employees come in, we will go through a full protocol of using thermal readers about temperature, et cetera, et cetera, hand wash. All that stuff, they'll be given. They'll have to sign the waiver of protocol that they understand what's needed. And one of the key things we have, and we're really focused on around doing that, is making sure that the experience when the employee comes into the office isn't as vastly different as it was before. It's going to be a little bit different and we're really focused on the tolerances from people, but it's so they don't come in and they'll have to wait half an hour just to get in the office.</p>

<p>David</p>	<p>I mean, that's such a valid point. And actually, one of the things that we've been grappling with is that ... I had a percentage of people who had to continue to work in the workplace because of the security issues, because of the fact that they were connected to a live bank, for example, or there was an underwriting engine that could only be accessed from the office and, therefore, we had to keep people there. One of the interesting things that we found, and Margarete, I will bring you in on this because I'd be interested to know what your views are on this. Actually, those workers who went through that ... I mean, 'Customer' used that example before about red to amber and that sort of amber plan. When that red plan hit and we all went into that. We said to a percentage of our colleagues, "Guys, I'm really sorry, but you're going to have to keep going back to the workplace."</p> <p>And we saw that sort of emotional curve of people having to go through that and worry about that and fret about that. And then, I guess, we're almost making adaptations in real time to that environment. But then the next wave came, which was really interesting, which I guess is 'Customers' amber wave, which is, we probably now need to start thinking about how we bring back some of those colleagues who were moved to the home and are now safe to come back. And we saw a really interesting thing where the people who remained working in the office environment were now actually starting to worry about the introduction of new colleagues coming back into the workplace because there was a fear about open spaces, there was a fear about crossing each other in the reception area.</p> <p>We're having to adapt in this new world and a world that we never even thought up before. I wonder, Margarete, in your case, what are you putting in? What are you seeing coming out that allows the continued state of the people who continue to work there, and that's important, but actually this new dynamic situation where old colleagues, who they've probably worked with for 20 years, are now coming back into the environment and there's this real heightened sense now of worry and concern?</p>
<p>Margarete</p>	<p>Yeah. I think you've touched on many really interesting kind of psychological points there about who's returning, who's not returning, how do you safeguard them? And lots of organisations are putting in temperature checking, thermal vision solution, so physical devices to how then Glenn touched on all of the social distancing that's been put in, the reconfiguration of real estate. How do we use it to drive creativity and productivity? And then there's a lot that are still really uncomfortable and, fair enough, that don't want to go back in and may never go back in. I think there's an element of how do we drive a culture that's going to be connected so that you don't have divide between those that return and</p>

	<p>those that remain out of the office? How do we drive that fluid kind of dynamic?</p> <p>And one of the things we have seen with this remote working is, this kind of flattening of cultures and hierarchies, as well. I think, psychologically and that emotional safety, we're seeing lots of new anxieties, but also opportunities to reshape how do we interface with one another, how do we collaborate as teams? But there's no silver bullet here, David, I think. I guess, 'Customer', from your perspective as an insurance company, it'd be great to get your thoughts around ... You mentioned that you guys are working remotely. How do you see the kind of policies around collaboration and how is that creativity going to be continued, moving forward?</p>
Customer	<p>So I think some of it's unknown in the sense that if you ... What do I mean by that? If you talk about existing projects, existing themes, then the productivity seems to be improved, it has gone up. People have got a bit of balance. I don't know exactly why. I think that's where the challenges come in because there are things that you can't necessarily achieve over ... I mean, don't get me wrong, the productivity, the collaboration tools are fantastic. It seems like good stuff, but there are things that you can't necessarily achieve as well virtually as you can in an office space, in a collaboration.</p> <p>That's what I mean about the unknown side of things. You need time before you could effectively measure what we consider to be productivity. And how do you start to put a price on the lack of eye contact, say, if you can get through the virtual, the lack of kind of a factor response, the subliminal stuff that's going on that you're picking up when you're in a room. I don't know. Maybe there's pheromones, the scent that you pick up that allows you to build rapport and things like that that you don't necessarily fully appreciate because we've taken it for granted. There're those things that are yet to uncover, I think.</p>
Margarete	<p>Yeah, absolutely. That's a brilliant point. We're doing some work with MIT at the moment in the US around the fact that, actually, we only communicate 10% by verbal communication.</p>
Customer	<p>That's it, yes.</p>
Margarete	<p>All that body language when you're on Zoom calls and you don't see each other, or on Teams calls, or whatever platform you're using. And so how do we connect more? And I think the use of AI and actually picking up intonation and body language will be something that probably these platforms will have to start building in more of. And we know MIT are really closely at the moment in an accelerated way to manage remote</p>

	<p>working over the next while. But you touch on a really good point, which is mental wellbeing and productivity and the risk of burnout remotely and how do we ... because we're all kind of on this hamster wheel right now and how do we balance this out? Because I think we all recognise there's been huge productivity. People have adapted well and we've surprised ourselves, as a nation. I could keep going, but I guess, can we sustain that in the longer term?</p> <p>Those that may not be as vocal or as extroverted on remote working calls, are they getting the same voice? Are we looking after them? Are we being inclusive?</p>
Customer	<p>Actually, one of the things we talked about with Gartner partners was that the home working scenario appears to be lending itself particularly well for introverts and extroverts are struggling a little more. They like the interaction. So do we do a Meyers Briggs or some personality thing for team building? I wonder if now there'll be a greater emphasis put on that kind of thing, as this situation develops and say, well, where we used to put the emphasis on particular things when it came to our people because they're fundamentally the things that get stuff done. I mean, you can talk about AI and machine learning, but someone has to put it in place. Someone maintains it, typically, unless ... I don't know. But maybe there it will be a shift in emphasis from people, policies, or the way we recruit or the type of people that we recruit where your DNI position actually then talks to character type rather than gender, faith, race, things like that.</p>
David	<p>I agree, I agree. I think it's very early and, back to Glenn's point before, certainly when we'd been looking at bringing people back into the workplace, the agreement was always that you had to be there because of the physical nature of the work that you did, but actually a very close second was that mental health, and that ... I mean, I quite like the whole sort of pheromone test to see how people are interacting, but actually, being in an environment where you enjoy being in an environment. And actually, that's not relevant to wage, or to race, or to anything. It's because people enjoy being in an environment where, notwithstanding there's got to be social distancing in place, but human beings enjoy interaction with human beings and that, in itself, can help with the productivity.</p> <p>This is a brilliant debate, I have to say. We're into the last sort of five minutes. Keen, I guess, to get closing thoughts from Margarete, I guess, in terms of what you're seeing and what you're doing and what you're thinking about in terms of bringing in to really enhance everything that we've just been talking about this morning there, which is about security, it's about safety, it's about productivity. It's about all of these things that</p>

	<p>are important, but actually it's about the workplace and the workforce, as well. So, any sort of closing thoughts from you on that?</p>
<p>Margarete</p>	<p>Well, I think you kind of just nailed it. To be honest with you, I think we're seeing that there's no silver bullet on this one. Every organisation is navigating it carefully and some are faster than others, some with greater, bolder leadership, but I think organisations certainly are looking at trying to implement the right technologies and sustain them for the long haul for remote working or hybrid working environments. Some of that's investment in physical infrastructure and reconfiguration of real estate and putting in the right kind of safety protocols. For instance really looking at the remote working practices and, instead of investing in the real estate, they're investing in technology now and putting in smarter technology. Things like greater security, but also arrange tools and workplace tools that are going to help them work faster and more agile and that kind of app development side to it.</p> <p>I think the other big shift we're seeing is a huge change around leadership beliefs. I think, 'Customer', you touched on it. How do we create a more inclusive working culture as part of this? How do we learn from this period of strife and how do we drive these sustained productivity measures so that we don't all feel the impacts of remote working and missing seeing our colleagues who, actually, we realise now are our close friends? So I think big kudos to the kind of conversation around leadership beliefs and changes. I think we need to talk about that more around flattening of hierarchy, way to focus on mental health, a bit of a shift around diversity and inclusion because we can be more inclusive now with remote working and we should make sure that we build that into any kind of future workforce models.</p> <p>So, yeah. Honestly, I really enjoyed the conversation. So thank you, David, for hosting this.</p>
<p>David</p>	<p>No, very good. Very good and some good summarised points there. Glenn, any sort of closing thoughts from you?</p>
<p>Glenn</p>	<p>The one point we didn't cover, which I didn't think we would because it's a bit of an elephant in the room, is the cost of change. And cash is king at the moment. Right? And how do we ... We have a whole load of assets that we're probably not using anymore that're sitting in an office that are probably getting cleaned maybe once a month for the foreseeable future, and probably won't be used. So there's a property piece and that's more of a longer-term focus depending on the leasing terms you have, but from a reusing assets or getting value out of those assets back is something that, I think, most companies should be looking at right now because a lot of things were repurposed and just repurposed doesn't mean dead.</p>

	<p>There's still value in there. And so how do we help customers maintain and get that value add? I think that's pretty much the only last few things, but to be honest, guys, this has been a fantastic conversation. I've really enjoyed this.</p>
<p>David</p>	<p>Thank you so much for your interaction, as well. I'm sure other colleagues on the call are sitting, enjoying the debate and enjoying the discussion, as well, of course, and there's a lot to learn. I'm fortunate that I look after six and a half thousand colleagues who run our big operations and our big financial services customer operations and security is never forgotten, but never forget the importance of the human being in all of this. Their security is important, of course. And the better we can make that environment, whether that's remote or whether that's agile, whether that's back in the workplace, it's our responsibility. It's a leadership responsibility to make sure that that's in a good place.</p> <p>I liked Glenn's view before about let's adopt the mentality of 'when', not 'if' in terms of attacks, in terms of people who will be endlessly trying to engage with infrastructure, with core services, with the data that could potentially be breached. And I think that's a really important point there, as well. I think the other point, as well, that Margarete made, which is really interesting, and I thought was quite healthy to think about, which is bring in some new caution and training around security, actually make that part of what an employee is there to understand the importance of that, as well. It's not just about the technology, it's about behaviours. It's about the importance of that integrity, as well, as an individual, the integrity that you have and power to you, as an employee on behalf of the organisation you work for.</p> <p>Kind of feels like we're never going to be back where we were. Glenn, you made the point about assets and buildings. I know we're certainly looking at that. But one thing, to touch on the point that 'Customer' made about that need for interaction, we're kind of moving to what we're calling a hope mentality. So, we might not have everyone back in the office. We might not have everyone back six days, five days a week, but what we are going to do is look at that asset opportunity where we can bring people in or we can make sure that there is a form of connection, as well, that continues to ensure that that human side continues along with, of course, workplace services that allow for that activity, allow for the flexibility between the home and the office environment, as well, which is really good.</p> <p>And I think, just closing on 'Customer's' point, which I really liked there, which is this kind of new world brings new emphasis that we should be thinking about behaviour ... the need for that emotional intelligence, that EQ rather than just the IQ. The IQ can be supported by the infrastructure and the IT and solutioning, but EQ is equally important. And I think we've</p>

	<p>got to continue to find a way to make sure that we connect those two things to ensure that our workforce and our customers and our customers' customers continue to get the service that they expect.</p> <p>But a huge thank you from me, certainly, to Margarete and to Glenn for your interaction, as well, but also to other colleagues who have joined us and taken the time to come along and hopefully enjoyed the debate and the discussion. Hopefully, there were some good learning points that came up from that.</p> <p>So, huge thank you from me, and please allow me to wish you an enjoyable rest of the day or evening, wherever you are, and thank you so much, indeed, for taking the time to attend.</p>
Customer	<p>One thing, David.</p> <p>I just want to share. For what it's worth, if anybody's on this call or wherever that is viewing this as a threat to what was the status quo and not viewing this as a massive opportunity, then they're coming at it in the wrong way.</p>
David	<p>Great point. Completely agree.</p>
Glenn	<p>Absolutely.</p>
David	<p>Completely agree. This is the opportunity. We were talking, Glenn, Margarete and I ... We were talking, before the call and we were just saying, for all the years that we've tried ... I was telling the guys, but I had the perilous job back in 1998 of trying to get us to sell data, and remote, and videoconferencing services around the world. No one was interested whereas, look, we're all on this e-call now, it's second nature and none of us even think about that now. So you're absolutely right. This is going to be a huge opportunity for not just individuals, but for organisations to have a look at that risk appetite, the way that they operate, the options that now exist as a result of being able to leverage the security, and the capability that comes in from partners like Dell Technologies, for example, but also that new way of working and that new operational expectation and that new risk appetite that we've all got.</p> <p>So I completely agree. I think, yeah, we've gone through the red and the amber, but the green certainly feels and looks like it should be opportunity-based rather than risk-based.</p>
Customer	<p>Yeah. It's just going to be a different green, right?</p>



David	Yeah, exactly, different shade of green, whatever that is. Guys, thank you so much, everyone, for your time. I hope you enjoy the rest of your day and great to catch up.
-------	---

If you would like to join a future Atos Connected Experience roundtable, please speak to your account manager.