**Interviewer** 0:11  
OK, so now I think we are recording right now.  
Yes.

**UPR2** 0:15  
Yeah.

**Interviewer** 0:16  
OK, so let's start from Section A and so section…first question is, which one does you your unit that you work for belongs to?

**UPR2** 0:28  
Yeah. So I work for a private cybersecurity provider, so we're uh, we're a provider of network cloud and also endpoint security products in the global arena.

**Interviewer** 0:45  
OK. And the second question, uh, what unit do you work for that?

**UPR2** 0:49  
I'm part of the sales organisation and I am one of the presales consultants.  
So I spend most of my time with some of our largest European customers and particularly in the UK, in Germany and also Switzerland mainly. And I helped them understand the value that they can get from deploying more of our technology.  
And we look at it through the context of financial value and also how we can help them reduce cybersecurity risk.

**Interviewer** 1:23  
Umm, OK. And then how long have you been working for this unit so far?

**UPR2** 1:30  
And so I've been there for about 18 months and then prior to that, I worked for [the name of a major global networking firm]. I spent about seven years working for them, doing a very similar role, and then prior to that, I spent a career in financial services. So I was actually on the…um…on the customer side before I went to…to vendor side.

**Interviewer** 1:52  
OK. And…and the…the question four, I think you've already answered that.  
So yeah, we'll yeah, we'll position do you hold within the year.

**UPR2** 2:00  
Yeah.

**Interviewer** 2:03  
So you said you are the umm.

**UPR2** 2:08  
At my yes, my…my title is umm I lead value creation in Europe and some value creation lead for…for Europe. And so as I mentioned, that's working with the major European headquartered accounts that that we've got.

**Interviewer** 2:26  
OK. And so yeah, the 5th question, what are your main responsibilities?

**UPR2** 2:33  
Yeah.  
So what I will do is…so I will lead…um…structured consultative presell and discussions and engagements with our customers. And working with them, I will understand particular pain points or challenges or issues that they may be facing across the security arena, but also in the enterprise networking space. And then, alongside colleagues from a technical perspective, we will propose new technical solutions to them to meet those requirements or fix those challenges that they've got. And then I will then develop a value case for the customer around that which will then focus in on improvements across financial risk and also sustainability.

**Interviewer** 3:22  
Umm, OK yeah. Thank you so much. So let's jump to section E yeah, since then section CD…BCD is not...It's not for you. So section E. So the first question is what. You can just answer based on your opinions. That's OK. So what are the major cyberattacks in the UK and what are the modus operandi and you can also give some examples.

**UPR2** 3:49  
Yeah.  
OK, I…I think so it there's…there's for most probably knows full ones obviously, but the ones that end up making it into the news and I think first and foremost I think from…from what we see and there's quite a lot of diversity in terms of the organisations that get attacked. There's different threat groups who then sit obviously behind those different types of attacks. One of…one of the most recent ones was a private sector company. Who do work with the UK Government called [the name of a private company that supplied the UK government]. Um…they were attacked by or allegedly attacked by a Russian state sponsored group and they were targeted because they were believed to have documentation and schematics on the physical security of one of the UK's nuclear submarine bases. Equally outside of the public sector private sector is a constant target, but the motivations of those attackers is...is largely different, moving from kind of, you know, moving from kind of espionage type attacks through to attacks which are more financially motivated and…and more extortion based.  
So I think notable ones that we've seen in the news this year are British Airways and boots, also the BBC. Across all of those what you saw was that data exfiltration, was the primary motivation and of the attackers.  
The reason they did that was to then demand a ransom from those organisations, and of course the threat therefore was that the data would be leaked and released if they…they didn't provide that. And so those, those are kind of the…the primary ones that, that, that, that are probably hit the news in the UK most recently. I think beyond that you know I'm…I'm sure on a day to day basis, there's organisations of…of many different sizes which are being attacked by attackers.  
The motivations will vary. The techniques will vary. The level of sophistication will vary as well, but I think really from what we see is for actually there's no organisation who's really immune to this. And I think any…any organisation is…is a target for it.  
And actually the…the threshold for being attacked I think is…is starting to reduce as well as the number of you know, crime, as a service type kits become available on the on the dark web. And it actually lowers the threshold for attackers in terms of skills and capabilities and resources that they've got. And I think by virtue of that, it also lowers the threshold for the types of brands that get hit as well.

**Interviewer** 6:56  
OK. Thank you. And you mentioned about the companies called Zone?

**UPR2** 7:02  
There's [the name of a private company that supplied the UK government].

**Interviewer** 7:06  
[the name of a private company that supplied the UK government].

**UPR2** 7:08  
And yeah. Yeah.

**Interviewer** 7:09  
OK, so I'll have a look.

**UPR2** 7:11  
So yeah, so fairly recent one. But I think they…they were…they were hit by a…a Russian state sponsored group because of the fact that they had, you know military grade type information that was uh presumably deemed to be important.

**Interviewer** 7:19  
Umm. OK, so I think it's also related to the umm question number three, because you talk about umm your…maybe your…the relationship with…between UK and Russia and so maybe that's one of the reasons.

**UPR2** 7:45  
Yeah.

**Interviewer** 7:48  
Umm UK…yeah…is targeted.

**UPR2** 7:49  
I would imagine so. And I think I think particularly at the moment with the you know and…and it's not just for UK, but many countries have been very publicly supporting Ukraine in the war against Russia.

**Interviewer** 7:50  
Yeah, it's it's targeted.  
Yes.

**UPR2** 8:06  
But I think the…the UK in particular, and again I'm cautious to not be too heavily guided by just what we see in our own news, but we do seem to be very prominent. And I would imagine as a consequence for UK would probably be sort of near, you know, near the top of the list for Russian state to be targeted and you know, and I've probably imagine alongside, you know, probably France and you know, perhaps to an extent Germany as well. But you know, by virtue of the weapons that you know, the constant supply of weapons, we seem to be supplies to Ukraine. And the probability is that we've elevated our prominence in terms of targets.

**Interviewer** 8:50  
OK. Yeah, the war between Ukraine and Russia.

**UPR2** 8:54  
Yeah.

**Interviewer** 8:54  
Yeah, it's interesting. It's also similar to the situation in my country, Taiwan, and is now not really the same, but you know, people say that or maybe and nowadays you can, maybe tomorrow it will be Taiwan cause we have the really, really complicated relationship with China. So it's kind of…

**UPR2** 9:17  
And it's a…it's a very it's a very worrying prospect.  
You know, seem much more worrying for…for the Taiwanese than…than perhaps that the…the British, but you know Taiwan is the semiconductor, you know, manufacturing out of…of the world.

**Interviewer** 9:32  
Yes, yes.

**UPR2** 9:34  
So you know a bit beyond…beyond the economic and the supply chain issues which would come for you know and primarily the…the people impacts which are which are paramount actually it would be highly damaging to the whole of the world just because of that one particular industry alone. So it is a worry. There's no doubt about it.

**Interviewer** 9:53  
Umm yeah.  
Exactly. Semiconductor is one of the biggest reasons that we’ve been targeted, and yes, especially from China. Yeah.

**UPR2** 10:05  
Yeah, I'm not surprised.

**Interviewer** 10:05  
And yeah, yeah. So, uh, so the second question is, umm, because you talk about, you know different organisation, different industry, they will have the different kind of cyber attacks.  
So in your opinion, what are the major targets of cyberattacks in the UK and what are the reasons?

**UPR2** 10:18  
Yeah.  
Mm-hmm.  
Yeah, I it it's sort of very, very similar to to…to what I mentioned a moment ago, I think, yeah, I think the, the, the major targets are…are every organisation.  
I think there's just more that…that rise to prominence than others, and I think it's by virtue of, A, the types of information they have or B, the brand identity that they've got. But again, it goes back to the for active groups that are out there.   
What their particular motivations are? What resources that they've got and…and also what level of risk and protection that's in place for them as well.  
So again, I think if you go back to some of the Russian groups, there's a there's a very low probability that a Russian state sponsored group is going to get extradited from Russia to the UK for a cyberattack. And I think as a…one gang with a with…a with a lead of their court, and [the name of gang leader who appeared on an international most-wanted list] who's on the FBI most wanted list.  
And he is making a mockery of that by virtue of the fact he's got T-shirts printed with his most wanted picture on it.   
And he's actually profiteering from being on the FBI most wanted this. But the point there is that he is so immune to prosecution by virtue of what he does, where he does it from and who he is sponsored by. That he's…he's infallible in…in that sense.  
So I think…I think by virtue of about what you've got is…you've got a lot of governmental organisations who will be targeted for…uh, espionage type reasons or private sector organisations with governmental contracts like [the name of a private company that supplied the UK government], I think there's also opportunity for governmental type disruption.

**Interviewer** 12:15  
Umm.

**UPR2** 12:23  
So in the UK, the Electoral Commission were targeted not too long ago.  
What's the motivation behind that? I'm not entirely sure, but was there potential for interference for democracy, possibly, possibly not.  
Umm. And then then again beyond the espionage type…type place you've got just straight up…umm…financial motivations and extortion. And extortion is driven particularly into private sector. And in the UK we aren't such a large manufacturer than what you see, for instance in…say, Germany or in Asia or to an extent within the US. But manufacturers are always a prime target for extortion and very prime target for extortion because they've got very low tolerance for downtime.

**Interviewer** 12:53  
Mm-hmm.

**UPR2** 13:16  
So if you've got a manufacturing facility which has been subject to a form of ransomware, maybe the control systems have been locked, encrypted.  
And is it as it may be, that becomes very damaging for an organisation and they're keen to get back to business as soon as possible. And so again, I think I think for the UK we're…we're very heavily dominant in the financial services industry. That's a very data centric business too and that's obviously ripe for extortion by virtue of stealing of data, encrypting of data and so forth.

**Interviewer** 13:54  
OK, so uh, most of the attacks like around like ransomwares and then, you know, like data…umm…breach, things like that and then…Do you think…What kind of industries are easily to targeted?

**UPR2** 14:15  
And it's good, it's good question. And I I'm not. I'm not sure it's industries that are particularly easy to target. I think it, I think it's still going.

**Interviewer** 14:30  
Or like popular.

**UPR2** 14:32  
Yeah, pop, pop, popular. I think…I think manufacturing is…is always going to be popular and…and…and is and is popular for…for the…the first reason I gave, which was there's a low tolerance for downtime.

**Interviewer** 14:36  
Umm.

**UPR2** 14:44  
But secondly, they've got the OT environment, so the operational technology environment where they're using often, control systems, applications, technology that is old. And it wasn't…It wasn't built to be, you know, secure from secure by design, so security becomes really an overlay and protective bubble where is intended to be wrapped around for manufacturing environment. And equally in those types of environments, the windows to deliver changes.  
So for instance, patching for instance upgrades, for instance, were placed with technologies, is very limited, you know it…it.  
You know, I've worked with manufacturing clients before where they have just one annual change window, you know. And if you, if you think about manufacturing in, in, in a couple of different contexts, one of those is pharmaceutical manufacturing.  
And actually there's a client I worked today with based in the US, um…the global pharmaceutical. They had, I think it from memory, it was a two days…So it's a one weekend change window every single year. And within a hold of that factory they had to deliver all of the upgrades that they needed to sustain them for that coming year because the cost of taking the site down to deliver an upgrade was very material to the profitability of that business.  
So if you consider the everyday, there's new vulnerabilities, there's new CVEs, there's new KVEs, so vulnerabilities where there's now a known exploit or available, I think that's growing at a stratospheric raise exponential the number of CVS and the number of exploited vulnerabilities which are there.  
So you could imagine for that type of environment whereby you've got one change window a year, you've got aging infrastructure that needs to be updated, whether that's control systems, networking, physical appliance based security and you've got systems that need patching, you could end up with quite a big workload.  
So I think by virtue of that, I think manufacturing is always a prime target.  
Uh, and I think any data rich organisation becomes a…becomes a prime target as well. And…and you look at what's been going on with some of the US hospitality brands and last couple of weeks of MGM Resorts and you've got Caesars Resorts as well.  
So I never focus here is on the UK, but if you just consider those in the context to it, you know, sees it as report it. They suffers a ransomware they paid around so, but they also lost a significant amount of data, which could be anything up to around about 65 million records of personal identifiable information.

**Interviewer** 17:27  
Umm.

**UPR2** 17:38  
So that includes things like the Social Security number, and this was for all of the umm member database that they've got there. So you think data which organisations where there's the opportunity to exfiltrate large amounts of data, even if it's encrypted now using it as a way to drive extortion is very, very lucrative. And I think the UK, Germany, the US, any of these countries that have got any organisations domiciled with big databases, particularly that contains PII (Personally identifiable information), will continue to be a target.

**Interviewer** 18:17  
OK. Thank you. And then let's move on to question three. So, umm, what are the factors affecting the cybersecurity in the UK and you can also give some examples. I think you’ve talked about, you know, the…the political issue.  
So are there any others factors?

**UPR2** 18:38  
Yeah, I think I think that I think that the political and we…we spoken quite a bit about al…already. I think…I think the…the other side of it is, is…is people. And…and I think there's people comes into…into two parts here.  
One is…one is skills gap. So this is around…um…trains, competent, capable people who have built a career or are looking to build a career in cybersecurity. So I've got a lot of the clients I work with are short staffed.

**Interviewer** 19:06  
Mm-hmm.

**UPR2** 19:11  
They don't have enough cybersecurity trained individuals who are able to support an ever growing and ever more complex organisation, and the complexity is stemmed by distribution of workforce. So people working from home people working from remotely, but also distribution of resources.

**Interviewer** 19:27  
Mm-hmm.

**UPR2** 19:32  
So applications residing across multiple different environments, public cloud, private cloud, SaaS, Internet and so forth. So what you've got is you've got, you've got, you've got organisations which are which are transforming, some at a very significant rate, some at a much slower rate. But that transformation is opening up the attack surface, and that wider attack surface requires more data, more telemetry, more observability. And what it's doing is it's generating more alerts, more things need to be investigated and there isn't an abundance of people who can who can respond to that.  
Now, although technology has become a more sophisticated and is able to, you know, identify fewer false positives, become more autonomous, there's still strong reluctance, understandably, for organisations to hand over control of their whole security protocol to systems and AI and machine learning.

**Interviewer** 20:33  
Yeah.

**UPR2** 20:33  
And by virtue of that, there's still a requirement to have analysts, and there just isn't enough capable individuals at the moment. So I think there's a whole piece around the skills gap that needs to be…be identified for IT professional professionals.  
But secondly, I think there's also education and the number one attack vector is still through social engineering and it has been for many years, and I think the probability is it will continue to be as well. And I think with the advent of now, what we're seeing with GenAI (Generative AI) , we're going to see a lot more sophisticated, a lot more phishing emails and contacts via social and impersonation, etcetera. And I think actually it's gonna…gonna accelerate that as…as an attack vector. So I think by virtue of that, whether you work for a large global brand, whether you work for a local entity, there needs to be a raised awareness of being able to identify things that just don't look right, that…that land of you.  
Because as soon as you click something, a payload maybe hidden in the file and they take you out to a nefarious website. Is it may be whatever it might be, there's the opportunity there for the initial access to undertake, will it all comes down to somebody having to do something such as clicking on something to…to…to what they receive. So I think education in the spaces is really important too.  
And I think the other thing then around cybersecurity is just the sheer complexity.  
And I think the complexity is driven by the widening attack surface.  
So again, you know more distribution of employees, more distribution of resources, more surfaces that…that needs to be protected.  
And what that means invariably is…is more technology, more products, more vendors, more data, more things that weren't designed to work together as one homogeneous system.   
And I think by virtue of that, you will end up with overlapping security capability or we will all you end up with gaps because you…you thought you had something for this protecting a particular edge. But actually it doesn't exist.

**Interviewer** 22:53  
OK. Thank you. So you talk about the skill gap and the education. And I would like to ask more about…do you think that the skill gaps is because people don't receive enough training or because for example like they don't have enough job opportunities, things like that?

**UPR2** 23:20  
And yeah, it's a good question. I'm not sure why. I'm not sure I know that the…the reason for it. I…I…I think I think it might just be. I…I think it might. I think it's transitory, number 1, I…I don't. I don't think the skills gap is…is…is here to stay.

**Interviewer** 23:37  
Umm.

**UPR2** 23:38  
I think there are jobs. I think…I think…I think the issue potentially could be is that technology is moving so quickly, uh, and actually the education or overhead is really, really quite significant and I don't know what programs exist for instance, in colleges, in universities, to have career paths that take people from secondary school level type education and develop them into, you know, professional cybersecurity analysts, architects, strategists and so forth. So I don't…I don't have a specific answer. But my…my assumption would be the jobs are there. This is more about people having a defined career path and training curriculum in place to be able to get there with, well, I suppose also with…with enough support at…at the same time too.

**Interviewer** 24:37  
Hmm.  
OK. Thank you. Then umm, that's move on to section F. So the first question is, So what techniques and services that you provide to your customers, you know in the field of cybersecurity?

**UPR2** 24:56  
Yep. OK. So the company I work for, we've got a very broad portfolio of security products. We've got products that provide network-based protection. We've got products that provide endpoint-based protection. We've got products that protect applications and cloud workloads. Um, we got protections at, you know, products that protect email and and…and so forth. So, and what what's important about those is that number one, there's a…a broad platform-based approach to protecting across different attack services. And…and…and secondly, those are designs work together as well.  
So the idea therefore being is that if one particular technology protecting and monitoring one part of your attack surface detect something, it can drive update and configuration and policy change across the whole of those connected systems.  
So it works as well.  
So first thing we do is we try and prevent attacks taking place in the first place and… But they do, you know, organisation is impenetrable to…to an attack. There's, there's always a point of weakness. And I think with enough perseverance, with enough resources, with enough motivation, those points of weakness will be found.  
So the other things that we do as well as we provide various types of monitoring type services. So we provide…um…I think this leans into the skills gap that I mentioned a moment ago. We provide a security operations centre as a service, so we provide a level one log triage service so that our customers don't need to monitor.

**Interviewer** 26:39  
Umm.

**UPR2** 26:49  
So for instance, monitoring a firewall logs, those will go into a data lake.  
That data lake is monitored by various algorithms that try and identify indicators of compromise, and if we identify something, we'll go on our customers and we'll give our customers some guidance on what preventative or corrective actions that they need to take. We also provide threat intelligence services, which is built into that.

**Interviewer** 27:19  
Mm-hmm.

**UPR2** 27:20  
We also provide our customers with incident response services as well.  
So in the case that they are suffering a breach and they are suffering an attack and we've got teams of people who can help our customers try and try and recover for those.  
So those are the kind of the official paid for services.  
But what we've also got from a presales perspective is we've got more of the consultative pre sales advisory services as well.  
So this is where we'll be working with our customers and making recommendations to them about what they can do to enhance their controls and how they can do that on a more cost effective basis.

**Interviewer** 27:59  
Mm-hmm.

**UPR2** 28:02  
And that's really the world that but I live in, which is and how do we help our customers identify which of the areas that present the greatest risk for them, from a attack surface perspective. How would we propose that they reduce that risk?  
What's the cost? What's the technology solution and what's the value? For the…for the…brings to the to them. So I suppose if you view there's some presales and advisory piece, but there's also the product and the services that sit behind it too.

**Interviewer** 28:36  
OK, it sounds like you provide like more comprehensive services. Like from protection, monitoring and then cyber threat intelligence. And also you do some investigation for them if they got attacked. And you also do some consultancy, you know, to give them advices on, OK, yeah, that's amazing.

**UPR2** 28:51  
Yes. Yeah. Correct.

**Interviewer** 29:03  
OK. So that's move on to question two.  
So question two is on. Yeah. What are the your major customers? Like which kind of industries or?

**UPR2** 29:18  
And yeah, so I I I probably can't name names, but would we we've I suppose if I sort of take…take a step back and I'm probably sort of answer the…the question better this way and the company I work for is the largest vendor by number of units shipped of firewalls in the world by virtue of that most global brands that you would recognize and also most national brands in the UK you would recognise are our customer of [the name of a private cybersecurity provider]. And the probability is that they've got a firewall from [the name of a private cybersecurity provider].

**Interviewer** 29:22  
Yeah.

**UPR2** 29:57  
Firewalls are just one of the things that we offer.  
As mentioned, we got very broad portfolio, but the core of our portfolio is…is a firewall. So in terms of industries, again we operate across all industries that exist.  
We've got very strong pedigree, particularly with a financial services industry, particularly within data centre environments. And the reason for that is just by the uniqueness of the hardware technology that that, that we offer is ability to have incredibly high through put be able to have line rate type inspection and a very…very cost effective if price point.  
So for you know, very high-volume environment, so such as data centres, there's a lot of our technology and deployed again financial services. But also we've got again very strong pedigree action and manufacturing space as well. So we've got a lot of protocols that we can recognise and to that's quite important for the manufacturing whereby they use a lot of unique protocols in those environments too.  
But whether it's financial services, manufacturing, retail, energy, you know, we've got customers where we've got infrastructure deployed on offshore oil rigs, wind farms, solar farms and so forth.  
So we…we operate across all that, I think it's fair to say that if you just sort of take a step back and think of major global brands, major UK brands, there's a good chance there one of our customers.

**Interviewer** 31:38  
OK. Thank you.  
Then the question three, it's about what are the major reason that your clients come to reach out to you?

**UPR2** 31:49  
I think I think the reason for that is, is number 1 some brands ultimately, you know ,we…we've got a very strong brand that that brand has…has been built up over a number of years and and…and what…what that brand is based on is reliability.  
Like I say, having unique, up-to-date, threatened intelligence, we are well regarded by IT analysts. So lots of garner and also forester in our field.  
And then the other bit to bring all of that together is also the cost angle that I mentioned as well. So again, [the name of a private cybersecurity provider] got very broad portfolio.

**Interviewer** 32:34  
Umm.

**UPR2** 32:34  
Uh, but the the the leading product for us is the network firewall and the network firewalls is not gonna go away any anytime soon and it's incredibly important to the overall security posture of of every organisation across the world. And…and we truly excel in that space. So that's kind of why they…they come to us.  
But of course what we've got is we've got is portfolio that supports our customers to try and help simplify their overall security estate. And I can't remember what…what the latest numbers are, but it wouldn't be uncommon for a, you know, a large enterprise type organisation to have anything between 50 to 75 possibly up to 100 different discrete and security technologies.

**Interviewer** 33:23  
Mm-hmm.

**UPR2** 33:23  
And then play there, and by virtue of having so many different technologies, you've got multiple skill sets that you need to develop. So going back to skill shortage as well, understanding network security, understanding endpoint security, understanding IT fundamentals is one part of that. But then you actually get into the application of it and actually delivering security services and monitoring and so forth.  
You need to understand the products as well.  
So what you have is you have a huge amount of products deployed in customer environments and they're on a journey to try and rationalise and consolidate those.  
And there's a notion that customers will go to a series of platforms. They won't go to a single platform for security. I don't think there's probably truthfully any organisation today that's got a comprehensive platform that protects across every single attack surface without level of capability. And I think the view is that organisations will move to a series of platforms. Uhm, so you have a reason why they come to us is because we can help them simplify and we can help them. We can help them simplify and what that really means is we can help them move to a point where by they've got fewer vendors, fewer different technologies in their environment.  
What that does for them is it simplifies the security policy because you can have one policy, but it's applied across multiple surfaces.  
You have fewer management platforms, you've got fewer training requirements, fewer skill sets to…to keep on top of. But also by virtue of that consolidation, bearings are very strong economic case as well as you can imagine, you start to negotiate, you know, one, two or three contracts for hold of your security estate versus fifty 75100 contracts, you start to drive some very significant economies of scale.  
And again, you know from…from my experience, you know I spend a lot of time talking to customers and there's always a trade-off around risk reduction and…and also cost.  
So I think I think what…what we're able to do and I think it's fairly unique, I think within this in a security space where able to offer our customers or platform that can protect on a very broad basis across multiple attacks services at a very compelling price point.  
So we can help them free up capital or operating expenses, repurpose that and drive a much richer security posture.

**Interviewer** 36:02  
OK, then I want to ask that so your clients, most of them, they come to reach out to you is because it's before…before they got attacked, they want to enhance their cybersecurity or most of them they come to reach out to you because…because they got attacked? Before or after?

**UPR2** 36:18  
Yeah. That it's pretty. It's pretty…pretty before pre attack.

**Interviewer** 36:30  
Mm-hmm.

**UPR2** 36:31  
Yeah. Yeah, we…we do get clients reach out to us who are due in and also experience an attack. But at our business is about trying to prevent it happening in the first place. We're…we're here to help if it does happen. But our goal is to try and stop it happening. So and you know 99.99% of what we do is all about prevention as opposed to response.

**Interviewer** 36:45  
Umm. OK. So it sounds like most of…um…business here and they have some basic awareness of cybersecurity. So that's why they come to you before they got attacked.  
Because they want to enhance their cybersecurity. Is that correct?

**UPR2** 37:15  
Absolutely correct.

**Interviewer** 37:15  
OK.

**UPR2** 37:17  
And it and it. And you know, I don't think it's necessarily about one they…they have to they need to they…they've got to protect their organisations.

**Interviewer** 37:22  
Umm. Mm-hmm.

**UPR2** 37:25  
So that you know, our…our customers, you know, and our…our competitors as well you know, we…we don't, you know, when our customers don't just work with us. They…they work with…with multiple vendors. But it's a very proactive conversation about helping them improve their controls ultimately.

**Interviewer** 37:43  
Hmm. OK. Thank you. Then so question four is about in your opinions and so in what aspect your customer are sufficient about, you know in the field of cybersecurity?

**UPR2** 38:00  
I think I think probably the…the…the main thing that stands out for…for me again just based on based on my experience is…is understanding the trade-off of umm, the budget allocation you've got for security and how you apply that to drive the greatest amount of security return that you can.  
Because although security and cybersecurity is…is critical to every single organisation, it doesn't come with an unlimited budget. And by virtue of that, there are trade-offs that need to be made,there are compromises that need to be made, and there are decisions that need to be to be made. And I think the…the greatest challenge for the sea says that we deal with right now is understanding…umm, where do we…what do we need to protect against. And therefore, what investment should be…be making because we can't afford to protect everything in a very wide and widening attack surface. And at the same time, all that does again is it introduces more vendors, more technology, more complexity.  
So I think for our customers that the big challenge is, is, is understanding where the risks are, how to mitigate and how do we do that to drive the greatest amount of financial return.

**Interviewer** 39:18  
Umm. Oh, OK. So if they don't fully understand, maybe they…they will not be willing to invest more money on that? Would that happen now?

**UPR2** 39:30  
I think I think I…I…I…I…I…I yes.

I think I think that could happen, but I think I think that's probably more likely is that they will make a decision to make an investment in a particular security technology that no doubt we'll deliver what they need it to deliver and want it to deliver.  
But it may not be the most important thing for the organisation about point in time and…and I think I think the challenge for our customers is understanding how do I prioritise the decisions I…I need to make and how do I therefore prioritise investment that…that comes with it because there's, you know, clearly not an infinite, but that you could probably name 40…50 different security and capabilities.

**Interviewer** 40:04  
Umm.

**UPR2** 40:19  
And the question then is, is well, which ones, which ones are more important than others and…and what drives that level of importance? So what's the probability that if I don't have this, I've got an open attack surface that can be exploited.

**Interviewer** 40:34  
Umm, OK, thank you. So then, then let's move on to the fifth question.  
So what are the common cyberattacks that you deal with? Like from your customers maybe?

**UPR2** 40:50  
Yeah.  
So I think I think it sort of comes back toto the same ones that we spoke about earlier. Ransomware is still highly prominent.

**Interviewer** 40:58  
Umm.

**UPR2** 40:59  
I think it's increased by way of its daresay sort of level of aggression and over the course of probably the last 12 to 18 months as well. And I and I think there's…there's sort of two, two angles to that. One is the implementation of wiper malware now. And we're seeing more of that. I think about it was born out of the…the Ukrainian Russian War, but the shared destructive nature of…of wiper malware in the sense that the conversation…well, the…message now that some organisations are receiving from attackers is not we've encrypted all of your data, pay some ransomware will encrypt or decrypt it. It's we've decrypted all of your data, pay some ransom in 20 minutes or we're wiping it. And you're never gonna get it back again. And what it does, of course, it raises the level of urgency, but it's placed on organisation in a time where actually it's pretty urgent already. So I think by…by virtue of…of…of that, I think there's a propensity we're gonna start to see more of that. And of course the next 12 to 24 months or so. And then…and then the other side of ransomware as well is…is the…um…pressure now that attackers place on organisations to place ransom by going to the subject to data has been stolen and and contacting the, likes of you and I, to say, we have attacked organisation ABC. We've stolen your data and you need to apply pressure to organisation ABC to pay ransom to us or we're going to publish your data.  
So you're also then seeing that happening as well alongside it. So that's kind of the primary motivation we see. I think there's still be espionage, which is probably not as perhaps widely documented as some of the financial motivations. And then I think the other, the other piece as well that that you see a lot of as well is the development of backdoors and and…and exploits into an organisation. And you'll…you'll see attack groups who will specialise in creating a backdoor, for instance, to a OT, um…manufacturing facility and stop there and then put that up for sale. And…and that's…and that's their objective is to create those backdoors into organisations, sell them on. So other threat actors can then exploit those for…for whatever means that they wish to exploit them for.

**Interviewer** 43:47  
Ohh OK, so most of them types…types of attack, ransomware and maybe espionage and backdoor?

**UPR2** 43:58  
Yeah. Yeah, so ransomware, wiper, malware, extortion, backdoors? Yeah.

**Interviewer** 44:05  
OK. Thank you. Hey so the 6th question is about because you said that, you know, like every cyber defence will be breached eventually. So…So what would you do after your defence has been broken through by the cyber attackers that what, what, what is the mechanism you provide?

**UPR2** 44:32  
I think I think the most important thing that any organisation could have is…is to have incident playbooks and…and…and having a process documented a way of working understood and people rehearsed and drilled in the execution of that. Because time is…time is of the essence with this. You know, as…as soon as that initial access has been gained, it can take literally seconds, maybe in some cases minutes, for lateral movement to take place. And…and I think I think therefore the most important thing is…is…is having number 1, visibility and monitoring applications and systems in place. So that detection is a speedy as it possibly can do, but ultimately what's gonna happen is that's gonna send off some alerts into their security operations center somewhere. And either…a…and unless is gonna…gonna pick that up, all them up, or potentially a playbook that's got some prescripted processes are gonna…it's gonna…it's gonna kick into play. But the most important thing there is is speed and and also trying to to then contain it. But I think again from…from a lot of the reports I read, but one thing that's cited and continuously around the ability to reduce the potential magnitude of a cyberattack is speed of response.

**Interviewer** 46:02  
Mm-hmm.

**UPR2** 46:04  
And what drives often speed of response is having instant response processes in place. People understanding what to do and…and people not looking, you know, left or right as it might be wondering, well, what do we do from here.

**Interviewer** 46:20  
OK. So visibility and monitoring and also the speed of response. There are the two keys here.

**UPR2** 46:29  
I yes, I think I think you…you need you need you need to you need to know what's happened, number one. So…so you have to have the visibility.  
You have to be able to have the awareness that we're under attack. Umm, a lot of attacks lay dormant, make and lay dormant for days, weeks and months before the detections even picked up. So the speed to detect an attack is absolutely critical. And then secondly, having the right processes the right procedures in place to know what to do once we've detected that an attack is in place and there's a lot of data actually. IBM produce a report each year and it's a…it's a great report on one of the things that they measure is the loss of a cyber attack by time to detect and also a couple of our competitors also do…do that as well. And there's a very strong correlation between the financial impact of the cyberattack and the time it's taken to detect and contain it.

**Interviewer** 47:36  
OK. OK, so let's move on to the question seven. So it's about the cyber resilience.  
So how do you describe and evaluate the cyber resilience of the techniques that you provide to your clients?

**UPR2** 47:57  
Umm and I I think. I think it's strong and I think it's also getting stronger as well.  
I I think there's…there's…there's two parts to this for me. One is around the efficacy of products that we provide. And then simply doing what it is that they're…they're advertised to do and doing it well. So I think I think one is you know how good actually is…is for product. But I think even before you get into the product and is it performing its function, I think the bit again it comes back to that is understanding what you are trying to protect against and what you plan to be resilient from.

**Interviewer** 48:34  
Mm-hmm.

**UPR2** 48:37  
So that one of the one of the growing practices that we've got here at the moment, this is a piece of work that I'm leading, is how we can take a threat intelligence that we have got and turn it into something actionable for our customers. Because you could go online and you could Google threat intelligence and you'll probably come up with 100, maybe 1000 different sources, a threat intelligence. Everybody seems to have threat intelligence. Everybody claims their threat intelligence is better than somebody else's, but I think what's hard for customers is knowing well, what do I listen to and more importantly, what do I take from it and…and what do I do.  
So what we're doing in that space is we're actually mapping our threat intelligence. And we do map our threat intelligence into the processes as defined by the MITRE attack framework that articulates how cyberattacks are performed. So what are the actual processes that attacker is doing.  
What we've therefore do with that is we can give our customers a clear view of what you need to protect against and what you would need to be resilient from.  
And I think that goes back to the…the topic where's discussed earlier, which is how do we help our customers prioritise where they need to focus their efforts. And it would be interesting actually.  
But the MITRE attack framework is got, I think he's got current got 227 different techniques, so you've got I think 14 tactics. Those 14 tactics have got 227 different techniques. And those techniques are then got thousands of subprocesses that attackers perform. And by virtue of putting a set of those together in a combination of those together, they're able to get into an organisation, escalate permissions, move laterally, find assets, and then take action on their objectives.  
And what we found actually our threat intelligence is that when an organisation is being attacked, 90% of what an attacker does only uses 10% of the techniques as documented by MITRE. And we see that through our threat intelligence. So to try and answer a question here, what…what we're doing is we're helping our customers prioritize and we're able to prioritise, help them prioritise based on real data, real threat intelligence that points and shines a spotlight and what are the things that they…they need to be most concerned about.  
And I think the answer is, look, they need to try and protect against everything. But reality is we don't have the…the funding. We don't have the budget to do that.  
We don't have the people, the time and resources to do that either, so we need to help our customers protect, prioritise. And we do that through the threat intelligence and leading them to the areas that need to be most concerned about and the areas that need to be most resilient to.

**Interviewer** 51:31  
OK, I heard about the…the MITRE attack framework before, but it's, I mean, it's shocking for me you said it's only 10% of the…the techniques they use, so it means that you have to have your customer to really…umm do to identify the specific area…umm for them to protect their data or do the cyber resilience work.

**UPR2** 51:55  
That that. Absolutely. And I and I think that's I think that's the challenge that that organisations face which is when…when we think about what we're vulnerable to, we've vulnerable to an attacker. But what an attacker is doing is they're putting together a set of very sophisticated, a set of coordinated process steps. Ultimately, in order to be able to execute their attack from an initial reconnaissance and outside in probing of an organisation through to initial access, through to lateral movement, through to privilege escalation, through to encrypting data and through to exfiltrating data, if that's what they're the motivation is, and all of that's documented in MITRE. But the problem with MITRE is, is there's just so much of it, and that's not MITRE’s fault. That's just a reflection of the different array of techniques that an attacker will use. And a challenge therefore, for a customer is…is   
If I use MITRE as a basis of what I need to protect against, which is what you need to protect against, well, where do I start?  
Because there's so much of it. So to how we're trying to help our customers become more resilient is that we marry our threat intelligence based that we pull back from our appliances that we actually see take place, which has got a geographical and also an industry lens to it and we can shine a spotlight on all of those 227 techniques in MITRE, and tell our customers which are the ones which are most commonly being used in what sort of volume. And what it does therefore is it helps them prioritise. Because you can't…they can't protect against everything.  
So what…what we're trying to help our customers with is, look, these are the ones you need to be most concerned about. You do need to worry about them all, but there's some you need to be more worried about than others and we can help you understand what those are. And we can help you understand what controls you could put in place to become very resilient against those types of processes.

**Interviewer** 54:10  
OK, then let's move on to next question. And I think Question 8, 9, 10 can be all answered together. And so in your opinions…so because you talk about the services that your company provide to the customer, then in the future, like in what aspect do you think you can advance or to make it better?

**UPR2** 54:37  
And it's…it's a good question I must.  
I haven't really got a got a point of view on it, but I think I think I think ultimately is more of a macro thing as opposed to kind of a, you know, product level insufficiency thing. I think I think the macro goal of the organisation is to continue to develop a platform-based approach to providing security to our customers globally that enables them to become more resilient.

**Interviewer** 55:03  
Umm.

**UPR2** 55:05  
It enables them to simplify there and security infrastructure and an architecture and do that on a more cost-effective basis. And…and I think what that does, it just means that there's a continual evolution of security technology. Threat intelligence becomes more advanced; new capabilities are introduced; older ways are phased out as it might be. But it's all about continuous evolution. Continuous evolution of the threatened intelligence that integrates security with network so that they become one homogeneous entity.

**Interviewer** 55:48   
OK. So you do have the platform right now, right?  
You just want to, um, make it better to have more functions, or maybe integrate it better, and to offer that to your customers.

**UPR2** 55:54  
Yeah. But…but yeah, but the the…the platform exists. You know, there's…there's 10s of thousands of customers across the…the world who use it, whether it's in its entirety or…or whether it's part. But it's just about continued evolution. It's about keeping up with advancements in techniques about adopting new technologies, deploying AI more at the edges as it may be, or, you know, whatever…whatever it may be, but it's just about continuous evolution and just trying to stay one step ahead.

**Interviewer** 56:36  
OK. Thank you. So let's move to the to Section G. So first question is, in your opinion, what do you think about the public private partnerships in terms of cybersecurity?  
Do you think it really helps to…help them to make the cybersecurity better.

**UPR2** 57:01  
And but I…I haven't got really any experience in, in, in a public private partnership space. I'm…I'm aware I'm aware of numerous entities that exist within UK public sector and also sharing communities, public to private. I think that the basis of a lot of those is around communities to provide thought leadership in terms of security strategy and also in terms of sharing of…of threat intelligence.  
And I don't really kind of have an opinion sort of either way about the effectiveness and…and the value that they bring, because I'm…I'm…I'm not involved, but to me it seems obvious that the more information about shared the better. I think the…I think the only concern, not concern actually, I think probably the only observation I might have is…is there's lots of voices in this space. There's lots of organisations, whether it's private, whether it's public, whether it's think tanks, there's a lot of people with a lot of commentary and a lot of opinion. And I think sometimes what that means is…is is hard to …hard to extract the important points and know who to listen to. So I suppose my summary would be and yeah, I…I think partnerships are really important just as long as we know who to listen to and we know who to look towards for the right types of guidance.

**Interviewer** 58:34  
OK. So mostly it's about information sharing, you know, between different parties and then….and you also mention about some difficulties to…to do this partnerships and then…um…I want to ask you about…because you said you…you don't have many…umm…Opinions about the…the partnership mechanism currently but, but it sounds like you think that the…the mechanism nowadays not that mature enough. Maybe they need some…some, umm approvement, sorry improvement, things like that.

**UPR2** 59:26  
I…I…I don't…I don't know if…if, if I'm honest, I'm not…I'm not tied into any…any public sector conversations around this. So I…I…I wouldn't want to say that they'd need more maturity in improvement because I…I…I really don't know. My…my…my…my point was more of a in principle partnerships make sense because it facilitates information sharing. That information enables action. My only caution is…is just making sure that the information is being shared as heard by people. There's not too much of it coming, and people can…can therefore act upon it. Otherwise it just becomes another voice in a very crowded space of voices.

**Interviewer** 1:00:13  
OK, then how about in [the name of a private cybersecurity provider]? Umm do you have some partnerships with the public sectors?

**UPR2** 1:00:22  
We've got, we've got a lot of public sector companies, not companies, organisations we…we work with where various colleagues of mine are security cleared to…to be able to do that. So we've got them as customers, but they're equally, we've got partnerships, I believe in the in the public sector space through information sharing.  
And I know there's the National Cyber Security Centre, which I think we do a lot of work with. I believe they offer a threat intelligence platform, the CISP, but I don't know the detail of what we do with the National Cyber Security Centre and then what, if anything, we share into a CISP platform.

**Interviewer** 1:01:04  
OK then. So if public sectors and private sectors they work together..umm, what do you think…like for example your company, what can you provide in this partnerships? And what do you think about the…the government, maybe the…the public sectors. What can they provide to make these partnerships better? Like in general, like. Yeah. What you what do you think about that?

**UPR2** 1:01:39  
I think…I think the…the most important thing, but the…the public and the private sector could…could do together is drive a program of…of skills and education., ultimately. I…I think you know the public, the sorry, the private sector has got so much investment, so many companies, so much insight and intelligence as to what's going on at any given point…point in time. And…and that's a contribution at that they can make. But again, it's that how do you…how do you manifest that and how do you make use of it, whether it's just…just simply so, so much. But I think…I think beyond all the about, I think the most important thing that partnership could focus on is education. And I think it goes back to making sure that for the longer term and the next generation, we've got proper…um…broad programs in place. It ought to generate a new wave of workforce with cybersecurity skills to…to be able to step into that field and help protect organisations. And then equally, I think there's a…a level of campaign that's needed around raising everybody's awareness and understanding of cybersecurity risk and just the…the simplicity of…of, …of how attacks often manifest, which is you received something, you clicked on it. So I think…I think that for me would be beware probably the most amount of tangible value that come from…from the partnership would be.

**Interviewer** 1:03:24  
OK, then how about…um…policies? Cause you know it's obvious that the government has the power to…um…to tailor the policy. But maybe sometimes it's not that it's not what…What we really need. So do you think this partnership maybe will help them to have a better policies or?

**UPR2** 1:03:47  
I think…I think, I think and I I'm not sure if there is a policy on this. But I think one of the areas where that we need policy on or enhance policy is around being able to identify what your major cyber risks are and being able to quantify them in a way that is able to put a monetary aspect behind the impact of that of that cyber risk manifesting. So you know what is the expected financial impact of a malware incident at British Gas, as an example. You know they they're provider of, you know, critical infrastructure as…as, as an example. But I, but I think I think having organisations and whether it's public or private and it should, it should be both having organisations been forced to really step back and consider cyberattacks, the risk that they provide or present to the organisation and being able to then really understand how those take place, how you control and protect against them and understanding the relationship of those to the purpose of that organisation and being able to force a mechanism in terms of you guys, you need to be able to put a number behind this. And I just think having…having that level of requirement will force organisations to become very…very precise around what cyber risks they face, what the impact of those are. And I think ultimately actually what it does do is I think it drives better decision making. And I think…I think better decision making, I should say to finish, drives greater resilience.

**Interviewer** 1:05:41  
Mm-hmm. OK, the better decision and then better cyber resilience, yeah, definitely.

**UPR2** 1:05:48  
Yeah, yeah.

**Interviewer** 1:05:49  
Ohh OK. And then I think, yeah, that's it for today. Yeah.

**UPR2** 1:05:55  
OK, alright.

**Interviewer** 1:05:56  
So yeah, that me press stop recording right now.