**Interviewer** 0:51  
Yeah, okay. So I think we are ready.  
And yeah, first. So thank you so much for agreeing…participating this interview. So, I'm going to start from Section A, OK? So, the first question…yeah…is which one does your unit that you work for belong to?

**UPR1**1:07  
Hmm..my… I work for a private cybersecurity vendor.

**Interviewer** 1:20  
OK. And the second question is what unit do you work for?

**UPR1**1:25  
Within that company, I work in the commercial unit, so sales and sort of customer interaction.

**Interviewer** 1:34  
Okay and then how long have you been working for this unit?

**UPR1**1:39  
I have just over 2 years, 2 and half years.

**Interviewer** 1:43  
2 and half years. OK. And then what position do you hold within the unit?

**UPR1**1:45  
Hmm…business development manager.

**Interviewer** 1:53  
Okay. And then what are your main responsibilities?

**UPR1**1:58  
So, it would be the sort of 360 sales cycle. So, um…finding new clients, finding pain points within those clients, getting them on boarded, resolving various different problems with them and basically trying to sort of sell my company services into those clients overseeing delivery of those projects. And then working with them afterwards or after the fact to remediate, improve and then sort of the cycle continues in terms of finding new opportunities and new projects to sell services.

**Interviewer** 2:38  
Ohh okay yeah, it sounds like a lot of work and.

**UPR1**2:42  
Yeah.

**Interviewer** 2:44  
OK. So that's just for the basic information. Then we'll just jump to section E.

**UPR1**2:51  
Hmm.

**Interviewer** 2:52  
Okay. So, the first question is, um, what are the major cyberattack in the UK, like in your opinion, and what are the modus operandi? And you can also give some examples.

**UPR1**3:05  
Yeah. So, I guess the…the main ones that we see are sort of most common would be ransomware. That's the sort of very particular. Ohh that's a very popular one at the moment.  
Um, they're particularly financially motivated, so we see sort of actors operating ransomware style attacks for…uh…for financial reward more than anything else.  
Then you've got a other sort of threat types, such as sort of malware which can have different sort of modus operandi. Again, there's sort of financial elements involved there, but it can also be sort of used in the sort of espionage….uh route as well. So, for actors in that might be considered sort of a…a espionage lead actors.  
Then we probably have another common one in the UK would be data breaches, so they have a more wide range in MO.

**Interviewer** 4:04  
Hmm.

**UPR1**4:10  
So, um…data breaches can be accidental, but something like 53% of data breaches in the UK in 2022 where as a result of just mistakes by people.  
Um, whether that's sort of…yeah…not removing an ex or putting an external recipient on an e-mail that contained sensitive information that would be considered that it is something as simple as that could be…would be considered a data breach. So yeah, you got accidental sort of human error. There's one of the reasons there.  
It probably is susceptible to both corporate and international espionage data breaches. So not only sort of from nation states and what have you and the your sort of China's, Russia's and…and the like, but also from other companies. So there are… there are all the companies always looking for ways to get sort of information on…on competitors etcetera. And again, financial motivations are another common reason for data breaches from loan or sort of individual actors. So, gaining access to certain forms of information can be leveraged.

**Interviewer** 5:02  
Hmm.

**UPR1**5:27  
Ohh…and sort of play back to…to the target organisation and then another one would, I guess, be sort of, yeah…the…the risk of an insider threats and that…that again is very really…or is a real sort of threat to corporate espionage and what have you. You see that with sort of disgruntled employees or sort of fired employees or sort of compromised employees.  
So yeah, I think that would probably wrap up these are main cyberattacks we sort of see.

**Interviewer** 6:03  
Hmm. OK. So, uh. Yeah, like ransomware. So, you said like the three key three keys. The first one is ransomware. And the second one is data breaches. And then insider threats?

**UPR1**6:16  
Yep.  
Um, I would. I would probably say the…the big three out of out of those four, the big three would be ransomware, data breaches and malware.

**Interviewer** 6:19  
These three, right? Malware, OK.

**UPR1**6:28  
They're the most… yeah, they're the most common. Insider threats do exist, but they are…they're…they're…they're much less common.

**Interviewer** 6:37  
OK, OK. I understand. Yeah. You…you also mentioned about some political factors. So yeah, maybe I would the following question may…

**UPR1**6:45  
Umm.

**Interviewer** 6:48  
Ohh there will some where you can like and like to explain more. Yeah, like Russia and China. And so yeah, I would like to ask… so…

**UPR1**6:54  
Yeah.

**Interviewer** 7:00  
Do you encounter a lot of attack that is government supported? Government supported, I mean.

 **UPR1**7:11  
Um, not actively, so the…the clients we work with aren't typically large enough or dealing with sensitive information to the extent that a nation state would be the direct targeter. However, there are and a number of clients that are subjects to attacks from people that are supported by nation state. So it's…it's maybe less so China in the UK, but in the UK there are definite examples of the Russian state enabling individual groups to target retail and financial clients in the UK.

**Interviewer** 7:58  
Hmm.

**UPR1**7:59  
So whilst there might not explicitly fund them or be directly behind the attacks, they will allow those organisations to operate and sort of turn a blind eye to it.

**Interviewer** 7:59  
OK. OK. Thank you.  
Then let's, um, go on to the second question. So then what are the major targets of cyberattack in the UK and what are the reasons? So this question is mainly about like for example like which industries or I don't know the government yeah, maybe industry, yeah.

**UPR1**8:40  
Yeah. So I think if.

**Interviewer** 8:43  
Yeah, things directly.

**UPR1**8:45  
Yeah, if…if you were to look at the statistics, I think, um.  
It varies. So the…the biggest targets, the most attractive targets would be your financial services or financial sort of institutions on the whole, because they are the ones that are gonna pay out the big sort of the big bucks, the…the most money…if they're breached. However, they are the most mature out of any organisations set in the UK.  
Um…In terms of what we see in terms of volumes of attacks, the most popular targets at the moment in the UK are the education sector, the charities sector and areas across the like the retail sector and that sort of publicly available information that you can get off the ICO website, the Information Commissioner's Office.  
I can send you a link to that. That's very good for statistics and it sort of shows you rankings of the number of sort of confirmed data breaches in each sector…each year.

**Interviewer** 10:01  
Okay, thank you.

**UPR1**10:05  
Yeah, I mean and…and the reason why they're targeted more at the moment is just…funding…an availability for funding uh cybersecurity services. So, I mentioned that like a the financial services are obviously the…the main or the like the…the golden target, but they've got a lot of money that they can invest in cybersecurity whereas these sort of charities sector, education sector they don't and those sort of sectors have contained personal a lot of personal information which can then be sort of compromised and sold on the on the black market.

**Interviewer** 10:43  
Hmm.  
OK, so the main reasons here are still like the…the economic reason, right? The money, then. OK. OK. And so then the third question is what are the factors affecting the cybersecurity in the UK? And you can also give some examples.

**UPR1**10:54  
Hmm. Yeah.  
So we talking from an attacking perspective or a defensive perspective here.  
So I think if we're looking at the attackers, what…what we would see in obviously I work in the private sector, so we're largely dealing with commercial clients etcetera, dealing with businesses very much the main motivator for attackers is financial gain and what they can financially gain from attacking a client.  
Um, and that's why I sort of ransomware is the…the biggest…um is the biggest sort of vector and…and I guess I've probably considered them the same, but maybe looping back to question one. You've got phishing as well, so phishing with a pH. I would kind of see that up in there as ransomware, but some people sort of consider it separately. But again, that's why ransomware and phishing are so popular in this in this country because, at least amongst sort of commercial clients, is because attackers wanna get money out of the targets they're hitting.  
And I guess answering question 3 from a um defence perspective, the main factors involved in cybersecurity here are risk mitigation. Ohh it's very much a cost benefit.  
Attitude is not like a…a nation state, or if you're dealing with a public sector things where there is large amounts of sort of public funds available. Here are a lot of clients are dealing with budgets, very sort of…strained budgets this year and trying to…get themselves in the most defensible position in the most cost-efficient way.

**Interviewer** 13:02  
Hmm.  
Yeah. OK. So then in addition to the financial gain?

**UPR1**13:10  
Hmm.

**Interviewer** 13:10  
Factor…And…Um, do you think there will be like other factors?

**UPR1**13:19  
There are a lesser extent, particularly in…in the retail section. I mean, if we're looking at things like IP loss or intellectual like theft of intellectual property. Some clients, particularly if you're in the maybe fin tech or in the sort of technologies spaces, IP is very much a...the sort a… after element.

And...and we see that sort of you. I mean you look at the…the Chinese auto market, right? A lot of the designs for those are arguably very similar to the IP of European carmakers that's probably been lifted and shifted at certain points. But it's that sort of, it's that sort of principle of if we're not talking financial gain, then we're talking a big motivator will be the intellectual property of the victim organisation.

**Interviewer** 14:09  
Hmm. OK.  
Then yeah, I actually went through the website of [the name of private cybersecurity vendor] I and um, your services including like it says is um…Sorry, let me check it's a PCI…PCI DSS it's a it's a standard…about the payment card industry, so you are most of most mostly um helping customer with this kind of uh stand issue and standard, right?

**UPR1**15:03  
Yes. So yeah, PCI is one of the sort of industry standards we help our clients align to.  
So I guess it kind of loops into your point on the the…the…the down section F about sort of .7, but yeah, in the UK we have a lot of formal standards around cybersecurity that help organisations… hmm… aligned to best practise and aligned to a level of best practise that fits their budget.  
And some of the the standards that we align to or help clients align to are PCI DSS like you mentioned, Cyber Essentials and Cyber Essentials Plus, that's the UK's sort of scheme that is designed to help organisations achieve a basic level of cybersecurity, so any sort of any organisation can go out and…and ideally achieve Cyber Essentials basis, whether that is a local bakery on your High Street up to um…I don't know…. I Pret A Manger (a name of a business) or some someone like that. And is designed to enable everyone to…to achieve it… at least a basic level of cybersecurity awareness and compliance across the business.

**Interviewer** 16:32  
Hmm.

**UPR1**16:33  
And…and other standards like ISO 27001. And what have you and…and…and that's where…those…those sort of standards we kind of use as benchmarks with clients to…uh… improve their resiliency.

**Interviewer** 16:51  
OK. I understand. Yeah. ISO 27001 is kind of international right cause in Taiwan we…we are introducing that too yeah.

**UPR1**17:04  
Ohh. Perfect yeah.  
So yeah, it's…it's quite a European standard, but it's good that yeah, it's good that…that's coming over in Taiwan as well. You might find another one called SOC 2… SOC number 2 pops up a lot because that's a…a very American focused standard. It's widespread across America. And I know there's sort of a lot of US influence in China and sort of Southeast Asia. So that might be a popular one that does sort of emerge over the next five years or so over there.

**Interviewer** 17:38  
OK, you said SOC 2, right, SOC 2. SOC.

**UPR1**17:41  
Yeah. SOC. And the number 2.

**Interviewer** 17:45  
Number 2 OK I will take a look of that after this. And so then let’s back to yeah section F and then the first question and it is what techniques and services that you provide to your customers in the field of cybersecurity?

**UPR1**18:05  
Yeah. So, I'll…I'll guess as we sort of spoke about there in terms of the standard. So, what [the name of private cybersecurity vendor] sort of operates in arguably three core sections.

**Interviewer** 18:15  
Hmm.

**UPR1**18:16  
One we called Technical Assurance, which focuses on…Like what the industry would call penetration testing and that is almost a…it is what effectively series of tests that assess the like the technical controls organisations have to sort of almost simulate what an attacker would do, simulate being a…a hacker or a…a…a bad actor and sort of letting organisations know where their technical gaps are across their infrastructure and networks, or their sort of applications, their cloud infrastructure, things like that. So, it's looking at things from a technical perspective.  
The other department is sort of advisory or…or…or sort of GRC. That's Governance Risk and Compliance and that is looking at things that are more widespread level looking at organisational policies and practises. And that is where as we sort of mentioned before alignment with standards comes in. So whether that is sort of Cyber Essentials, ISO, SOC 2 etcetera and PCI is making sure organisations are complying with their relevant standards.  
And then we have the…the audit side of the business, which is almost sort of not siloed off, but it…it, it has sort of walls put up around it for good reason where we can go in and perform the formal audit and self-edification of our clients against these standards if these standards have a certification requirements.

**Interviewer** 19:46  
Ohh. Okay.

**UPR1**20:13  
So PCI DSS and ISO 27001 are both at the same time a information security standard, but also a certification. So that's where sort of audit and our GRC department separate.  
We we're not marking our own homework effectively and you'll find that with a lot of organisations that do both, they can help you achieve compliance with that standard and their audit department will be completely separate and allow you to sort of not mark your own homework when you…when you check them on that.

**Interviewer** 20:48  
Hmm. OK, thank you.  
Then the second question is then who are your major customers? But I don't mean you have to give me the names of the customers. I mean like the which industry or maybe government things like that?

**UPR1**21:06  
Yeah. So yeah, I'll in terms like I can sort share our industry wise and…and we're sort of cross industry based. So we have a lot of retail clients, insurers, financial services, etcetera. So we're…generalist is the wrong word, but we have good experience across a broad range of the UK sort of service industries.  
And yeah, I think obviously with our history is a PCI DSS sort of assessor. We've obviously got a lot of heavy experience with organisations that process payments like merchants and service providers. So hence the sort of strong presence in the retail space.

**Interviewer** 21:56  
Okay then do you also have um, some customer…customers from the public sectors maybe?

**UPR1**22:04  
We do have customers that interact with the public sectors and we are sort of part of various and it'll will probably be something that we are come down to in the section G but we do interact with the government and with public sectors.

**Interviewer** 22:14   
Hmm.

**UPR1**22:19  
Um, and we do have extensive interaction with government funded organisations so almost at hybrid style ones.  
We don't extensively deal with government departments because they can be quite slow and…you…you need…almost….extent, like almost too burdensome….uh certifications at points, so it's often only the big…it's often big cybersecurity companies like the your…NCC is or to that level that are on the trusted sort of providers for or like essentials (Cyber Essentials) and stuff like that…that have cyber departments big private consultancy companies they often swallow up a lot of the government…Um tenders.

**Interviewer** 23:28  
Hmm.

**UPR1**23:30  
So yeah, it, in short, we…we do work with government departments, but not…not exclusively. And they wouldn't sort of sit anywhere near the top of…our top client lists.

**Interviewer** 23:44  
Okay so most of them are like still from like private business?

**UPR1**23:50  
Yeah, I mean.

**Interviewer** 23:50  
Most of your customers.

**UPR1**23:52  
Yeah, even the government departments or even the government sort of affiliated companies we work for would still be considered private businesses. They're still registered as private business on…on Companies House.

**Interviewer** 24:04  
OK.

**UPR1**24:04  
They just have element or they just have funding streams that can sometimes originate from government.

**Interviewer** 24:11  
OK, OK, I got it. And then the…the third question is, so what are the major reasons that your customer come to…to reach out to you…to you?.. yeah.

**UPR1**24:27  
Yeah. So, for us, we were a consultancy. So, we…we don't necessarily sell cybersecurity products. So, customers come to us when they either have a need for formal auditing, whether that's PCI DSS, ISO 27001, etcetera. That will be a reason why they come to us. We're on accredited lists for that. So, our company name appears near the top of those lists, we're often more above the top of those lists as well.

**Interviewer** 24:35  
Hmm.

**UPR1**24:56  
Um, but they also come to us first of external support. So, where they've either got had the realisation that they need to mature in terms of their cybersecurity resiliency, they might reach out to us or we might reached out to them and sort of made them aware of that gap in their organisation and…That's where we sort of have engaged with them with our services.

**Interviewer** 25:24  
OK, so most of your customers, they reach out to you after the incident happened or?

**UPR1**25:34  
No. So, we're…we're the other way around. So, and there's something that I've sort of bring up later on in here. We don't have a response side of the business or we do, but it's not our…it's not our…it's not our MO, our MO is operating pre…largely pre incident. So, our aim is to build our clients resiliency to sort of recognise weaknesses within the client, build them up so those are no longer weaknesses and sort of recognise more etcetera, whilst also accrediting them for necessary standards. So for example like you mentioned, PCI DSS that's an annual requirement for clients to be audited against that if they want to take payments in the UK.  
So they often clients that have only just found out about that standard or only realised that they…they have that requirement will look on the PCI DSS Council for a list of providers or a list of auditors, and that's where we'll they'll reach out to us.

**Interviewer** 26:24  
Okay.

**UPR1**26:42  
There's…there's numerous ways that we sort of engage with these clients, but yeah, that…that's largely it. We are pre incident and our aim is to…improve clients resiliency so that they don't…ideally don't get hit with a with an incident, and if they do, the impact of that incident is…is minimalised.

**Interviewer** 27:06  
OK, I see. So, if so, you're basically doing the pre incident job. But after the…if they…they encounter the incident, maybe they will seek help from…to other cybersecurity firms maybe?

**UPR1**27:24  
Yeah. So, I mean, if…if…if they're a client of ours, they'll probably reach out to it like so we…we do offer like first responder services, if any, if our clients are signed up to that get breached, we can offer initial support, but we would then bring in a third party that specialises in…um…incident response remediation, wash up and digital forensics that's a…a very different service line to…to the Black… the rest of [the name of private cybersecurity vendor] as a…as a company.

**Interviewer** 27:54  
Hmm. OKOK, thank you.  
Then the…the 4th question is in what aspect do you think that your customers are insufficient the most?  
Like that, of course, in the field of cybersecurity.

**UPR1**28:17  
Yeah, I think what we see across the industry is just resourcing. So, a lot of our clients have the resource and budget, I guess go hand in hand.  
A lot of our clients, they there, there's a genuine desire to improve, they want to improve their cybersecurity… posture. A lot of them just don't have the hand like the available people to action all of the information that is getting fed into that department. So, [the name of private cybersecurity vendor] would be one of a number of cybersecurity vendors that these customers are working with and each one of those vendors will be providing this department with actions to…to do, to improve their sort of cyber posture, and that's where we sort of see clients sometimes get swamped is just not having enough hands or enough bodies to…to…to do the work.  
And that goes hand in hand with budget, because in order to get more that resource…human resource, you need more you need like tens of or hundreds of thousands of pounds more budget, which isn't always available.

**Interviewer** 29:33  
Hmm. OK, so most of the reasons are, um, the budget concerns, right? for your customers.

**UPR1**29:41  
Yeah. And I think that you…that would be the…the case.

**Interviewer** 29:45  
Hmm.

**UPR1**29:45  
Everywhere I think. Um...I think there's a…a growing understanding around the country around Europe, etcetera of the risks of cybersecurity. It's just bringing up budget from your, your board or your company is sort of funding mechanism to…to deal with that and that is probably the biggest blocker most organisations have.

**Interviewer** 29:58  
Hmm…Yeah. OK. Thank you. Then…um…how about the like…  
How would you describe or evaluate your customer's cybersecurity awareness and concept?

**UPR1**30:28  
Um...good question. I think it…it depends…on the client, so clients that we work with or that I work with, we sort of do annual reviews, etcetera and we…we try and educate them.  
Um, I guess the best way of from an outsider looking in being able to understand and organisations own understanding of cybersecurity is their compliance with different certifications. So, an organisation that has ISO 27001 and more often than not, these companies will list that on their website.  
Um...a company that is also 27001 accredited, you know will have a pretty good understanding of…of…Information security and governance.

**Interviewer** 31:24  
Hmm.

**UPR1**31:24  
I think it is quite generic and it's quite difficult to paint everyone with the same brush. But, if you were to be an outsider looking in, the best way of understanding an organisations understanding of cybersecurity is the level of standard that they comply to.

**Interviewer** 31:47  
Okay so.  
So do you think that, you know, like the government is trying to put more policies or the, you know, the certificate? So, this way will help the…this business to grow their awareness?

**UPR1**32:05  
I…I think so. I think that's one of the motives of Cyber Essentials Plus and I guess the the NCSC, the National Cybersecurity Centre. Um…I would say it's not…a government… well… personally, a government policy level. I don't think it's the most…I don't think it's being drilled into people enough. I think the…the public and the…the…the UK public's probably main interaction with cybersecurity is when their e-mail… when they're Hotmail or whatever, e-mail account is repeatedly getting spammed or they're getting sort of scam calls etcetera. I don't think the government is maybe doing enough to educate people.  
Yeah, I think a corporate level, I think there is a drive from the NCSC to get people engaged. I think there's sort of an…organiser, particular organisations that want to work with the UK Government or UK Government affiliated organisations, you need to have things like Cyber Essentials Plus. So, putting that requirement onto companies forces them to engage with cybersecurity improvements.

**Interviewer** 33:23  
Ohh, OK…OK. I see. Then let's move on to the…the 5th question. So…  
But maybe that….maybe the question five and six is not, not for you to answer, right? Cause you said you are, um, more….um, yeah, dealing with them…

**UPR1**33:43  
Yeah, I think I would, I would...I mean, yeah, five, I think five links back to the first question we…we answered. But six I guess I can give a bit of an answer there in a sense that…so, we don't set the defence really. We…well…. I guess we do we sort of set up guidelines on…on how to deal with that if they breakthrough the…the defences. So, this is where penetration testing is a useful tool. So…

**Interviewer** 34:02  
Hmm.

**UPR1**34:13  
Um…as context, most penetration testing is done with the thing called whitelisting put in place, so organisations will have firewalls and various what we call first line of defences in place. So where if you're testing the web app it will have like a web application philtre.  
Um, when penetration is done often to make best value out of best value for money, you asked the client to turn those off for the duration of the pen test. Now that means that the result…the…the findings or sort the results of the report are indicative of…what an attacker would find if they got through that first layer of defence.  
So, you could say that penetration tests are a good way of the harm reduction, because they've done on the assumption that you've got through that initial…defence mechanism.

**Interviewer** 35:15  
Hmm. Okay.

**UPR1**35:17  
That and then in addition to that, from a from a governance perspective, you say sort of incident management now from a…a governance perspective, we encourage every organisation we work with to have what's called a instant response plan.

**Interviewer** 35:18  
OK. Hmm.

**UPR1**35:33  
And that is a…a set of actions that organisations or a document that contains a set of actions that the organisation has got signed off at board level and has an understanding of that in the event of an incident, they follow those steps so that everyone is sort of uniform. They're all singing from the same hymn sheet.

**Interviewer** 35:56  
Hmmm. OK, so you just said something interesting. You said the board level. So do you think um…is it a key to…to like to make this board level personnel to have more awareness or like more focus on the cybersecurity?

**UPR1**36:19  
For sure. Yeah. I mean, if we…we always say this mantra of [the name of private cybersecurity vendor], if you're not, if your board isn't engaged with your cybersecurity strategy, then it's not going to go particularly far. The Board of the People that are signing off your budget, the board of the people that are ultimately the financial and organisational driver of the...or facilitator of your cybersecurity strategy.  
If you're it, it doesn't throw the will in the world that you, you might have as a head of IT to implement a strategy, etcetera. If your board aren't in agreement with you, that strategy won't go very far and we…we know that from experience with our clients. So yeah, absolutely, getting the board on board with your…objectives, the reasoning behind it…um…is…is key. And I think sometimes that's the issue that organisations have is…your head of IT will be talking in technical terms, and it's often in a…a…in a language that the board doesn't necessarily also speak. Boards are very focused on financial or financials, on numbers, on impact to business, whereas head of IT might be looking at things from a technical perspective and when they…they relay to their board, there's often a miscommunication and I guess that's sometimes where organisations like [the name of private cybersecurity vendor] come in and…and help bridge that gap.

**Interviewer** 37:57  
Okay…I See.  
And then let's move on to question 7. And since you talk about your help your customer to maintain or enhance the cyber resilience and maybe you can talk about more about that, like how would you evaluate this kind of service you provide to your customers?

**UPR1**38:21  
Yeah, so good way of evaluating sort of compliance is sort of soft auditing in a…in a…in a sense. If a client has desires to achieve Cyber Essentials Plus for example, you can soft audit, then you can sort of check their progress against the individual. So, these standards are almost like a list of controls like 27A or like it's just are they doing this sort of thing very much a list of questions and you can tick.  
They're sort of level of compliance, so if you want to sort of see where your clients sit in terms of resiliency, you would do a…an exercise very similar to that. You can do baselining exercises with them. Now that varies from consultancy to consultancy, how they carry those out. And I can't go into too much detail about how we would do something like that. But you can…you can perform baselining exercises against clients.

**Interviewer** 39:24  
OK…Then let's move on to, I think Question 8,9 and 10 can be answered together since they are talking about it the same thing. So, I just want to ask that in what aspect do you think like your services, which aspect you want you think is insufficient and you want to improve and how would you like to improve?

**UPR1**39:40  
Hmm…I guess um.  
From a from a delivery or from a availability perspective, I think an organisation like [the name of private cybersecurity vendor] as a sort of mentioned we don't have a an in House response capability. Now that would be the obvious...Um…String to add to our boat to sort of make it a complete it…complete in house offering. Now unfortunately that is a very expensive though in building a response team is an incredibly expensive endeavour. So, I can understand why we utilise sort of third party partners for that instead. So, I guess for me that would be the only insufficiency. I guess from a technical perspective, all our departments…um…are aligned to their own industry best practise standard whether that's sort of CREST with the technical assurance team…um for the…the PCI QSA (Qualified Security Assessors) being considered sort of senior important figures on the PCI Council. So, from a technical delivery perspective, we don't really have any insufficiencies. From a service provision perspective, it would be nice to have a response team, but as I mentioned, that's a very expensive…um…thing to…to set up.

**Interviewer** 41:20  
Ohh, okay I see. So you…um, it mean that you want…you still want to do like more comprehensive service to the you know in terms of cybersecurity, but because it's expensive, so you now you have the cooperation with you know different companies like you know every company has their own…um…specialty so you can work together?

**UPR1**41:46  
Yeah. Exactly that. Yeah. Um, in a sense. Yeah. But it would be nice for us to be able to do the whole sort of 360 life cycle of cybersecurity management. But, with that 4th part of response is yeah is…better for us, as an organisation for where we are, to utilise trusted third parties are for the moment.

**Interviewer** 42:14  
Okay. Thank you. Then let's a move on to Section G. Section G is about the private public private partnerships. So, the first question is, um, what do you think about the idea of public private partnerships in terms of cybersecurity?

**UPR1**42:33  
I think they've…they've got the.

**Interviewer** 42:33  
And you think that's helpful?

**UPR1**42:36  
Yeah, I mean, it's definitely got its got its place.  
And as an organisation where engaged in various government or public sector frameworks etcetera, to keep us engaged with different sort of public departments, um, I think, and I think on the whole that process is not outdated. But, it's quite difficult to see the wood from the trees in terms of that. And I think it is very much geared up to large corporations. So at least from a commercial perspective, um, it's very difficult sometimes to compete with…large cybersecurity organisations, when it comes to winning a commercial tenders…in terms of wider information share…Information sharing partnerships.  
But, we as an organisation...with involved heavily with CREST, sort of the technical assurance sort of standard for…for testing. However, that's not entirely public sector. That was a sort of private sector set up that was adopted by...though was approved by the NCSC. So, I think…for public sector, I think the private sector definitely does drive improvement and does definitely…does drive engagement more so than the public sector.

**Interviewer** 44:09  
Hmm. OK then,,,then as you know and you know in the UK, have you heard about, you know like some cases or experience the really like public and private partnerships maybe like in terms of I don't know training or like policy making or to investigate case things like that?

**UPR1**44:35  
So I think if you look over in, there's…there's things over in like [the name of a UK cybersecurity hub] and sort of cybersecurity hubs etcetera and [the name of a UK cybersecurity hub] is one of them where there is a lot of public sector engagement there. Unfortunately, it's all very confidential and the…the research hubs and the…the research hubs and the policy like interaction with policy making is very difficult for most people that work in the sector to understand what's going on over there is incredibly confidential…and…quite hush-hush in terms of what's going on. Personally, I don't know much about…so any ongoing collaboration projects between the government and private sector when it comes to policy or…or research, unfortunately.

**Interviewer** 45:27  
Hmm…ohh…that's OK. But you did mention about. Sorry. Yeah, please keep on.

**UPR1**45:31  
So yeah, it's a set.  
When I was going to say I for…for the for the most part for Section G, it's not really a strong suit of mine because at least with [the name of private cybersecurity vendor] we…we are very heavily privately.  
Sort of focused. So….um…we don't have a research arm within our company. The…the internal research we do is largely privately led and attached to different accreditation bodies that we're affiliated with.  
Yeah, you…you…you are gonna mention something that the odd mentioned around public private partnership.

**Interviewer** 46:16  
Yeah, that's OK then uh, if, uh, [the name of private cybersecurity vendor] doesn't have that kind of mechanisms but you can answer these question like based on what you know about, you know, the entire of UK.

**UPR1**46:26  
Hmm.

**Interviewer** 46:31  
Yeah. So, I was going to ask because you mentioned about information sharing. So, do you think that is the, it's a good way to, you know, to pub…this public private partnership like we can do on this direction?

**UPR1**46:52  
I think so, but I think by a large it would be a…a one way. It'll be a largely one way direction in terms of information sharing and that would be private sector into public sector because the private sector has…multiple sort of factors...or multiple degrees worth of more data than the public sector. And so, is largely unrealistic because the private sector has no incentive to share...into the public sector without funding. So that's where one of the limits is.  
I think…there's also...yeah, it…it sort of the…the use of the information as well. I think the…I think there's definite like reticence from the public…uh…from the private sector to overly share into the public sector.

**Interviewer** 47:49  
Hmm…OK, I understand. So may... Do you think that maybe more incentive…incentives will make the private sector more willing to more willing to cooperate…cooperate with the government?

**UPR1**48:08  
Yeah, I think so. I think you private sector companies are always incentivised by money, right? And like we sort of mentioned that the big organisations, you big consultancies here, you're Essentials etcetera will have a wealth more…a wealth of information that they can share and…and they do share with their…with their...contractual partners.  
Yeah, I mean, organisations within government departments that work with these sort of big four companies, they regularly lean on…on those consultancies for subject matter expert advice. But yeah, a wider level, I think the government would need to find a way of incentivising these organisations to do a bit more widespread information sharing.

**Interviewer** 49:00  
Hmm...Okay. Then what kind of incentive do you think will boost the willingness?

**UPR1**49:08  
Tax breaks…probably something like that. Um.

**Interviewer** 49:11  
Hmm.

**UPR1**49:12  
It would have to be a largely you would, well, the cynic in me. And so it would have to be financial incentives for them to…to…to really engage.

**Interviewer** 49:19  
Hmm.  
Okay, so should be financial?

**UPR1**49:23  
Oh, oh, yeah. Financial. Yeah. Yeah. Financial or contractual, in…incentives, I mean, you can always dangle the carrot of a tender in front of a big organisation, I guess. But yeah, really, to make it the most clean you've gotta…is probably just gotta be a tax breaks and stuff.

**Interviewer** 49:43  
Ohh okay so then I want to ask that if you know the public private partnership is really working right now. What's strength do you think that the public sector can bring on this cooperation?

**UPR1**50:04  
I think.

**Interviewer** 50:04  
And also from the private sector too.

**UPR1**50:07  
Yeah, I think the…the…the public sector has the at least in the UK with the sort of intelligence forces, their…their...their degrees of information share that will help from the…nation state perspective.  
Unfortunately, I think I don't know. I think my…under my personal understanding of it is that the private sector is…leaps and bounds in terms of cybersecurity awareness etcetera, etcetera is leaps and bounds ahead of sort of at least UK government cyber capabilities.  
Ohh, a macro level. I mean there's not information…there's not a huge amount of information sharing between different private consultancies. So, that's where the…the public sector probably has its strengths is that…information sharing within its own entity.

But if you were to look at…the private sector as a whole, I mean threat intelligence. You the threat intelligence company is out there are probably like such as you…you recorded futures, etcetera or similar will probably have more information available to them as a collective than any government does…oh… maybe China and the USA.  
Your consultancies have a wealth of subject matter experts across them…on the whole, that'll be again, if you to look at the private sector as a collective, the wealth of knowledge and capability there far exceeds that of the public sector. Plus the pay is better in private sector. So, your best minds are filtering out into private.  
Um, the limitations of private is that knowledge and capability can often be siloed into individual organisations rather than across a collective.

**Interviewer** 52:04  
OK so. Um…my last question is…cause it sounds like you most like you have the.  
And most mostly negative…um, feedback on this public private partnership because you think it's not that real…realistic, is that right? And.

**UPR1**52:27  
Yeah. Yeah. I wouldn't say maybe negative, but I would have probably agree with you there that…engagement of public private level on a widespread basis is largely unrealistic, I mean…It's slow enough, particularly in regards to policy. The government hasn't massively been listening to the private sector regards to the sort of Online Protection Bill (Online Safety Bill) and stuff like that. And you find that the cybersecurity company is a suggesting things that aren't…are suggesting things to ministers that aren't being listened to.   
Yeah. And lobby groups are opposing sort of some suggestions. You…you've got cybersecurity firms at odds with…um big service providers like Google and what have you. So…cybersecurity unfortunately isn't a revenue generating…business is a security the business. So, we're often at odds with…things like I don't know...cookies for example, are on…the like cookie policy with Google etcetera. There the cybersecurity industry was at odds with that because what we…what we're saying is from a security perspective needs to happen. Google don't want to happen at all cause that would horrifically damage their business model and their yeah their business model. So, that's kind of the difficulty that cybersecurity has is that we take a…safety first approach and…opposing big business often doesn't.

**Interviewer** 54:17  
Okay then um.  
In your opinion, what can be improved in terms of public private partnerships?

**UPR1**54:29  
I think.

**Interviewer** 54:29  
If we want to do that yet.

**UPR1**54:31  
Yeah, I think if…if cybersecurity was really sort of felt like it was engaged and had a proper…And had a…a…a more vocal voice at the table, then I think they'd be…more interest in public private partnerships from security…cybersecurity firms.  
Today, that's not necessarily felt like it's happened. At least that's the sort of narrative that you sort of see within information security forums, etcetera.  
So I think at the moment…the engagement doesn't necessarily seem like it achieves anything, so therefore sort of engagement wanes.

**Interviewer** 55:13  
OK…Then I think that's it, yeah.

**UPR1**55:19  
Perfect. Well, yeah.

**Interviewer** 55:20  
So yeah, that. Yeah, that's the. Yeah. Yeah. I think you you just gave me a lot of information. Yeah. So thank you so much. Yeah.

**UPR1**55:22  
Hopefully that helps.  
Yeah.  
No worries. Yeah, hopefully any other questions you have sort of let me know and I'll answer if if I can. There's obviously somethings that are commercially and technically sensitive on on some of these subjects, but yeah, like a done today where I can happy to sort of answer any follow-ups.

**Interviewer** 55:30  
And.  
Okay, thank you so much. So let me just stop…recording right now.