0:0:7.890 --> 0:0:10.180  
Interviewer  
Uh, so I'll start from section A.

0:0:10.190 --> 0:0:13.920  
Interviewer  
Section A is for just basic information.

0:0:14.230 --> 0:0:19.760  
Interviewer  
So for the first first question I will put you in private cybersecurity providers.

0:0:20.210 --> 0:0:23.540  
Interviewer  
And so let's go to second question.

0:0:23.550 --> 0:0:25.450  
Interviewer  
So what unit do you work for?

0:0:26.540 --> 0:0:34.430  
UPR4  
OK, I when you say you're not, so I work for an I'm an owner of [the name of a cyber security firm]. Uh, I'll. We've been accompanied since 2011, 2011 and we, I'm the business development director, but I'm also NCSC head cybersecurity consultants, so I've been a cybersecurity consultant for 20 years.

0:0:58.960 --> 0:1:1.820  
UPR4  
I main responsibilities within the company.

0:1:2.510 --> 0:1:6.450  
UPR4  
Uh, obviously identifying and finding new business.

0:1:7.570 --> 0:1:7.910  
Interviewer  
Umm.

0:1:7.420 --> 0:1:33.460  
UPR4  
I appealing on delivering proposals, but I also do mentoring for my staff to make sure that you, obviously they…they…they understand and quality control on any of the work that people do as well, but I also do cybersecurity consultancy where I deliver strategic guidance to boards and like a virtual CISO type roles. Uh, I and run large projects. So that's…that's kind of my sort of area of responsibility.

0:1:42.30 --> 0:1:46.240  
Interviewer  
OK, so 20 years is really long time, so you must be really experienced.

0:1:47.400 --> 0:1:47.890  
UPR4  
Yeah.

0:1:47.900 --> 0:1:48.350  
UPR4  
Well, what?

0:1:53.950 --> 0:1:54.180  
Interviewer  
Umm.

0:1:48.360 --> 0:1:58.530  
UPR4  
What keeps saying is I've been doing it before it was called Cyber, so I did it when I was in the [the name of a national navy] as an engineer and then came out and became a civilian. So yeah, a long time.

0:2:1.230 --> 0:2:5.180  
Interviewer  
OK, so I think you just answer all of the questions in Section A.

0:2:5.230 --> 0:2:14.390  
Interviewer  
So let's jump to section E so it's section E the question section E are more like comprehensive questions about the cybersecurity. So the first question is when in your opinion and what are…what are the major cyberattacks in the UK and what are the modus operandi and you can also give some examples.

0:2:33.500 --> 0:2:33.950  
UPR4  
OK.

0:2:33.960 --> 0:2:34.930  
UPR4  
Yeah, no problem at all.

0:2:34.940 --> 0:2:49.980  
UPR4  
So ransomware is always is is a is a big a big issue and and and continues to be I primarily I think because it's there's a lot of criminal gangs out there and and they see it as an opportunity to to make money.

0:2:50.650 --> 0:2:52.40  
UPR4  
I mean examples. I can go back to sort of the WannaCry back in 2017. I think that was, which was the UK's National Health Service, get hit quite badly with that and that was that was down to, I think, the exploited a vulnerability in in the in the operating system in that case. So it was that the rationale behind that was that the…the NHS hadn't kept their systems up to date, so that they were left vulnerable.

0:3:20.890 --> 0:3:31.340  
UPR4  
Another one is probably more recent, which was uh, which the UK Electoral Commission, where they…they lost. Well, well, I think there was about 30 or 40 million instances of personal data was left, was capable to be exploited. And that was basically just down to the fact that they hadn't patched something. So it goes back to doing sort of the basics of cyber correctly. So somebody got, and presumably via through…through the Exchange Server. I think it was and exploited the records that way, but if they'd have met the requirements for the UK sort of Cyber Essentials scheme which deals with five basic controls.

0:4:13.700 --> 0:4:14.720  
UPR4  
Firewalls, secure configuration, malware protection, vulnerability management security aware, updated effectively, and user access controls that wouldn't have happened really.

0:4:40.450 --> 0:4:40.900  
Interviewer  
Umm.

0:4:28.260 --> 0:4:41.720  
UPR4  
So that that's kind of the main ones we've there's other breaches out there, you know over the years where you've had British Airways lost half a million customer records or something to try to steal it. I talked…talked another one back in 2015.

0:4:47.280 --> 0:5:0.480  
UPR4  
You've also got the potential electoral…electoral tampering in the United Kingdom, but that it's…it's what we…it’s a cyber attack because you're trying to manipulate social media. But it's not what we would…it's not sort of the thing that we would deal with. It's…it's…it's too, it's we…we deal with standard cybersecurity controls and frameworks etcetera.

0:5:12.740 --> 0:5:18.200  
UPR4  
So is that enough for you, or do you need do you want to ask me some questions or?

0:5:19.70 --> 0:5:19.680  
Interviewer  
Yeah.

0:5:19.730 --> 0:5:22.20  
Interviewer  
So yeah, I think that's enough.

0:5:23.810 --> 0:5:23.990  
UPR4  
Yeah.

0:5:22.30 --> 0:5:31.560  
Interviewer  
So ransomware is the biggest and in addition to ransomware, do you have some, some other type of cyberattacks?

0:5:33.320 --> 0:5:38.130  
UPR4  
And we've, we've seen sort of attempted denial of service attacks. We…we see that quite often and normally they're mitigated quite easily by, you know, implementation of a web application firewall and we were working for a gambling platform provider, which would…which had a very sort of immature cybersecurity, and they didn't have something like that. Now you know. So they did then ended up denial of service attack, but we…we implemented a WAF or recommended the implemented a WAF and that took that away.

0:6:13.610 --> 0:6:27.80  
UPR4  
Other standard, sort of, whether they're cybersecurity is just the general users, you know, making mistakes and sending information to the wrong people. Uh, not that can be through to lack of awareness or clicking on an email that's related to a phishing attack, which then feeds through into your ransomware attack and it's all it's all connected.

0:6:41.230 --> 0:6:42.160  
Interviewer  
OK. And let's go to question number 2. So question is about what are the major targets of cyberattacks in the UK and also what are the reasons?

0:6:55.400 --> 0:6:56.10  
UPR4  
OK. Yes. So that so in the UK then they're probably the major sectors for attacker sort of financial sectors and healthcare sectors.

0:7:8.80 --> 0:7:16.710  
UPR4  
At the moment, obviously with the…the increased threat from…from Russia, you're…you're seeing more on sort of critical national infrastructure areas. So healthcare, financial services looking at it from a UK Government perspective, the reasons for that are to a with the criminal gangs involved is to make money through ransomware attacks. But if it's from a nation state actor it is to impact on the people's confidence in the UK citizens confidence in the…the UK infrastructure. Yeah. So from that perspective.

0:7:55.790 --> 0:8:7.320   
Interviewer  
OK, so the motivations behind is, um, either like, uh financial gains and or the for some you say the national actors. So it's more like to manipulate people anything.

0:8:12.980 --> 0:8:17.860  
UPR4  
Yeah, manipulate people and to you. You know it. It becomes more of a political act than an actual because cyber cybercrime attacks because they can hide behind it because it's very, very difficult to prosecute. It's very difficult to trace back. It's not like it's not like a real physical attack, so hence the reason why nation state actors tend to use them through either their…their own units or their…their criminal proxies.

0:8:50.270 --> 0:8:50.670  
Interviewer  
OK. Then let's go to question number three. And So what are the factors affecting the whole cybersecurity in the UK and you can also give some examples.

0:9:3.140 --> 0:9:3.990  
UPR4  
OK, sure. Yeah, so. It's not, not necessarily related to the UK, but it's…it's an evolving threat landscape. It's constantly changing cybersecurity. There's always. It's…it's difficult to keep the…the attackers or, I'm not gonna say one step ahead, but they will always be developing new methods and technologies to exploit vulnerabilities.

0:9:31.100 --> 0:9:35.810  
UPR4  
Uh, you know, so we've got malware is becoming more sophisticated. You've got the use of AI, which is improved the quality of the phishing, the language and the phishing emails, for example. Uh, so that that's one thing digital transformation is another…another area. Companies are becoming more digitized.

0:9:55.530 --> 0:10:6.830  
UPR4  
Yeah, you know, we've worked with barristers firms in London that effectively up until 3-4 years ago had everything on paper and the most they would send was an email, you know. Uh, OK, but now the they're starting to digitize all their legal records so that that gives a…a larger attack surface to the to the cyber criminal or the cyber attacker.

0:10:20.10 --> 0:10:22.670  
UPR4  
Another area I suppose is quite important. It's an area that we find we struggle with this skills shortage is finding people with the…the skills and the mindset. Um, there's a skills gap, you know, finding trained people and it's very, very expensive to bring somebody in for certainly from our perspective as a small consultancy and train them up because they then move on somewhere else.

0:10:50.170 --> 0:10:51.0  
UPR4  
Yeah.

0:10:51.10 --> 0:10:58.900  
UPR4  
So it maybe it comes so skills shortage and but it's not just the skills shortage in the…the private sector and the public sector because they're not the best players. So if you're working for an NHS Trust or something like that, you can go out and work for a consultancy or a different firm and earn more money. So skills, skills, shortages is one. Uh, regulatory environment, I suppose that there doesn't seem to be…when people…that doesn't seem to be a lot of consequences to the individual if they've or…or the company if there has been a security breach.

0:11:32.550 --> 0:11:45.60  
UPR4  
Uh, I know you've got GDPR, but if if you think that the amount of security breaches there are amount, I think they're saying one in four UK companies that are breached. And, but how many of those have actually been prosecuted? Because they haven't looked after the data correctly. Certainly not one in four.

0:11:54.290 --> 0:12:13.130  
UPR4  
So the regulatory environment, even though it's stronger, could do with…do with probably a more stricter compliance regime to…to implement it to make sure that companies and governments protect the data that they've been entrusted with.

0:12:14.400 --> 0:12:15.890  
UPR4  
Uh, what else?

0:12:16.260 --> 0:12:17.410  
UPR4  
Supply chain attacks. I suppose there's another…another area that's…that's important and we do we do quite a lot of supply chain assessments for some of our larger clients to go and make sure that they're actually delivering a proportional amount of cyber of security for…for the information they they…they manage.

0:12:39.120 --> 0:12:43.600  
UPR4  
And say so, and one of the angles attackers are there. They're attacking the supply chain to get to the get to the end, their end goal and client as well, which I think was which said one of the classics, where was the…the espionage. The for the F35 fighter with British Aerospace and the Chinese nation state, stole the plans. Few quite a few years ago.

0:13:8.160 --> 0:13:8.400  
Interviewer  
Yeah.

0:13:7.40 --> 0:13:8.920  
UPR4  
So anything else on that?

0:13:10.930 --> 0:13:11.430  
Interviewer  
Thank you. That's a lot of information. Thank you so much.

0:13:14.210 --> 0:13:14.820  
UPR4  
That's OK.

0:13:14.620 --> 0:13:14.880  
Interviewer  
Yeah.

0:13:16.150 --> 0:13:28.40  
Interviewer  
So uh, I I can hear you talk about a lot of like for some like skill shortage and maybe the cybersecurity awareness and then the mindset.

0:13:28.130 --> 0:13:30.350  
Interviewer  
So I think it's linked to the question.

0:13:31.70 --> 0:13:31.890  
Interviewer  
Uh.

0:13:33.500 --> 0:13:33.800  
UPR4  
OK.

0:13:31.930 --> 0:13:36.40  
Interviewer  
Later, at which that I'm going to ask you about.

0:13:37.10 --> 0:13:37.530  
UPR4  
No worries.

0:13:36.50 --> 0:13:42.340  
Interviewer  
So yeah, that's that's uh, go to section F right now.

0:13:42.590 --> 0:13:50.540  
Interviewer  
And so section F is more like the the…the service you provide about…about the cyber defence strategy.

0:13:51.10 --> 0:13:59.560  
Interviewer  
So the first question is, what techniques and the services that you provide to your customers in the field of cybersecurity and yeah.

0:14:0.90 --> 0:14:0.660  
UPR4  
OK.

0:14:0.750 --> 0:14:0.950  
UPR4  
Yeah.

0:14:0.960 --> 0:14:1.550  
UPR4  
No problem.

0:14:1.590 --> 0:14:3.860  
UPR4  
Uh, so more, more of a sales pitch then. Yeah.

0:14:5.630 --> 0:14:5.980  
UPR4  
Yeah.

0:14:5.990 --> 0:14:6.300  
UPR4  
No.

0:14:6.550 --> 0:14:7.200  
UPR4  
So what...As we we're…we're cybersecurity consultancy, we…we…we sell knowledge based services, we've only just started going into doing products.

0:14:18.750 --> 0:14:26.140  
UPR4  
So we're…we're just we're qualis managed service provider and we're just getting our first contract. But the services that we provide are we…we do cybersecurity risk management. So we will go into a company, understand how that company works. Do a risk assessment, so understand what they're what, they're what's…what's their important assets, what they're important services are. Uh, identify any vulnerabilities or threats against that and then work out a threat mitigation strategy, you know, work out what's the what the impact is and what controls that we could use to actually implement that.

0:15:3.130 --> 0:15:5.740  
UPR4  
Uh, we also do penetration testing. So we will go in to a company and do ethically hack them. We're Crest certified company. So we follow the Crest guidelines for that.

0:15:16.930 --> 0:15:27.790  
UPR4  
So we'll do that on infrastructure, external testing and we have application, API, uh, Wi-Fi. Ohh and we'll do code reviews as well, so we'll go ahead and do, you know, for companies that have maybe created bespoke code to make sure that there's no backdoors left in there and I'm looking to see if they've actually created their code securely because if they've not put in a good…or a robust code and policy you know how to write on a secure manner code you know coders will just write what they want to make it work.

0:15:57.440 --> 0:15:58.350  
UPR4  
So so that. We also provide strategic services, so like virtual seesaw, virtual chief Information Security officer. So we'll go and I'll sit on a board somewhere and help inform the strategy, because people with our level of experience are very expensive for a company to bring in full time. So if we do maybe four or five days a month for a company, we can, we can act as a sort of a force multiplier.

0:16:30.960 --> 0:16:35.210  
UPR4  
On that perspective, we do standards, cybersecurity standards, so we will, we're Cyber Essentials Plus certifying body. So we'll go into a company and assist them through the Cyber Essentials process and assess them for Cyber Essentials Plus. So they'll get their cyber essentials plus badge, and that means that they should be protected against 80% of the standard sort of Internet born type threats.

0:17:0.660 --> 0:17:8.350  
UPR4  
Uh, Cyber Essentials Plus is good, but it's not good for a dedicated and motivated threat actor. You know if…if they want, you know, it's…it's really just to try and remove the…the noise and the bots, you know that…that potentially be attacking a company.

0:17:21.140 --> 0:17:23.430  
UPR4  
And what else do we do?

0:17:23.520 --> 0:17:26.890  
UPR4  
Security architecture, so we will come in and help design. So we work with and, uh, a technical provider and make sure that the security architecture around their…their…their system or their Services is…is created correctly.

0:17:42.10 --> 0:17:51.940  
UPR4  
We are actually, NCSC assured, for those services, so we've actually had to go through a process with the NCSC to make sure they were fit for purpose.

0:17:52.230 --> 0:17:55.280  
UPR4  
I think that's about it really.

0:17:55.940 --> 0:17:57.330  
Interviewer  
OK, that's a lot.

0:17:57.340 --> 0:18:10.480  
Interviewer  
It sounds like your services are really comprehensive from the risk assessment and to the defence and maybe to like after attack you also do some umm.

0:18:10.340 --> 0:18:16.50  
UPR4  
We'll…we'll do a bit of incident list so we would…we're not really an incident response company. So we don't have the, we don't have people on retainer waiting for something to happen. But what…We'll go in is we'll work with one of our partners who are…and we will go in and put an improvement plan and help the client so it doesn't happen again.

0:18:33.740 --> 0:18:34.250  
UPR4  
Yeah.

0:18:34.10 --> 0:18:36.620  
Interviewer  
Umm, OK, OK.

0:18:34.320 --> 0:18:37.30  
UPR4  
So what we'll do that here we don't. But we don't have a SOC. We don't do anything like that, so we don't do any 24/7 monitoring. We're…we're purely consultancy and management consultancy, basically.

0:18:46.730 --> 0:18:47.430  
Interviewer  
OK, OK.

0:18:47.520 --> 0:18:48.610  
Interviewer  
I I see.

0:18:48.840 --> 0:18:53.770  
Interviewer  
And so now question number two is who are your major customers? You don't need to give me the names, just maybe some industry or governmental institution, yeah.

0:19:0.970 --> 0:19:3.80  
UPR4  
No, no, no problem at all.

0:19:3.90 --> 0:19:10.100  
UPR4  
So so we've we started off as a purely sort of working with government. So we've worked with. I mean, if you go on a website, you'll see you'll see everybody that we've kind of worked with. I tend not to put current customers on there because it's historical, so we've worked with the Foreign and Commonwealth Office, uh Department of Transport, HS2, MOD, uh, Ministry of Justice, Uh Cabinet Office. You, you name it, pretty much most of UK governments, large agencies and departments.

0:19:44.230 --> 0:19:48.700  
UPR4  
From a personal perspective, I've worked with the MOD. I've worked with the security and intelligence services, so I've worked across all that. From a commercial perspective, we we've never really nailed down a specific sector we work in, so we've worked across a lot of different types of clients and the different sizes from small fintech startups, medical startups to large barristers, practices or firms in London.

0:20:19.270 --> 0:20:19.530  
UPR4  
Uh. We also do work for one of the largest mobile phone manufacturers in the world, where we do their third party sort of supply reassessment stuff. We also do work for one of the largest toy manufacturers in the world, so a real mix of clients, you know.

0:20:42.490 --> 0:20:49.400  
Interviewer  
So ummm from governmental to private sectors, like across all of the, OK.

0:20:50.80 --> 0:20:50.940  
UPR4  
Basically, yeah.

0:20:51.670 --> 0:20:52.440  
Interviewer  
OK.

0:20:52.550 --> 0:20:53.620  
Interviewer  
And that's…that's good. It means that you have a lot of experience of knowing what they need and what to protect.

0:21:0.880 --> 0:21:10.950  
Interviewer  
OK, so and number three question number three is so when your customers come to seek for your service and what are the major reasons?

0:21:12.310 --> 0:21:22.110  
UPR4  
I think I think part of the reasons are that the…we are a…we're…we're certified, we are an NCSC assured company. So we've been the…The NCSC obviously is the UK's National Authority, so…so with that, so. So it's about quality and getting people who are experienced in the field. Most of our consultants have got over sort of 10 to 15 years experience, you know and obviously we bring younger people through. So it's probably that. We've been doing it.

0:21:45.190 --> 0:21:50.480  
UPR4  
It's a company for…for like 13 years and…and we're an independent. So we don't, we don't, we've never really sold many appliances, so, so they get independent advice. It's not…It's not like going to um…going to Cisco and…and asking for security consultancy and then they try and sell you firewalls, you know so.

0:22:7.480 --> 0:22:10.80  
Interviewer  
Umm OK.

0:22:10.150 --> 0:22:13.200  
Interviewer  
And I have one more question for you.

0:22:13.370 --> 0:22:26.950  
Interviewer  
So when the customers they they come to ask for your service, normally it's most of them is before…before they got attacked or after that?

0:22:28.150 --> 0:22:33.620  
UPR4  
It's normally it's normally before, so they'll be looking to improve their cybersecurity. You know, they might want to… One that I didn't say, we also do ISO 27001 implementation. So we'll help implement an IMS (Integrated Management System) for…for a company as well. So yeah, the normal looking to improve or they're looking to get a certificate. So 27001 or Cyber Essentials Plus or they may need to have their annual pen test because they…they work with a larger company and they need to ensure that…that company's asked them for, you know, for verification that their…their systems are secure.

0:23:17.110 --> 0:23:17.590  
Interviewer  
OK.

0:23:18.830 --> 0:23:21.200  
Interviewer  
And let's go to question number four. And so in what aspect do you think that your customers are insufficient the most in the field of cybersecurity?

0:23:31.120 --> 0:23:46.100  
UPR4  
A probably the the…the lack of understanding of the of this threat. It…it comes down to it, will never happen to me. I think in a lot of cases and I and I don't think they, they understand that that's probably part of it. So it's an educational piece, I think. I think they…they don't understand a lot of them don't understand that, you know, this is this is a good thing to do and…and what you have to remember is if you're dealing with commercial organizations, it's all about money and translating.

0:24:11.920 --> 0:24:22.930  
UPR4  
It's very, very difficult to translate to somebody that if they get attacked, they might lose so many thousands of pounds because the attacks never happened. It's not like having a car where you have to be insured. And you don't have to be insured so they don't see it that way, so.

0:24:31.830 --> 0:24:33.800  
Interviewer  
OK, so most…uh, the major reason could be that they don't understand it, and also those maybe the awareness. They don't really umm…understand how important it is or…

0:24:47.340 --> 0:24:47.710  
UPR4  
Yeah…and…and…and the lack of lack of consequences I think, is what I said earlier on. You know, it's a lot or so the…the lack of personal consequences or corporate consequences that they're quite they're quite weak, really. There's plenty of companies that are still going after massive security breaches and yeah, you know, so and…and even the fines don't really relate that that much.

0:25:15.510 --> 0:25:15.890  
Interviewer  
OK.

0:25:18.200 --> 0:25:20.830   
Interviewer  
So then let's go to question number five.

0:25:21.130 --> 0:25:25.0  
Interviewer  
And So what are the common cyberattacks that you deal with?

0:25:27.310 --> 0:26:5.490  
UPR4  
So we would know we, as I say before we, we tend to go in sort of before to try and mitigate that any attacks so, so but the the, the standard attacks you know ransomware so you make sure that they've got a good business continuity plan and they're backups are sorted phishing we would look to obviously make sure that and that you have the good rule sets on your on your external sort of email and proxy servers but also education uh virus standard sort of virus attacks and it comes down to getting the basics right, you know. So your antivirus and you're vulnerability management systems, etcetera.

0:26:10.380 --> 0:26:10.930  
Interviewer  
Umm.

0:26:9.950 --> 0:26:13.660  
UPR4  
So we tend, we tend not to deal with them.

0:26:13.670 --> 0:26:16.970  
UPR4  
We trying prevent. It is probably…we we're more that the front end of it from that perspective.

0:26:24.250 --> 0:26:31.780  
Interviewer  
So yeah, and I understand that you said you are you are doing more like before like consultancy. So when you do the risk assessment, what are the most, uh vulnerability that you you've seen on your customers?

0:26:43.290 --> 0:26:44.710  
UPR4  
Ohh that can be most of it depends on the maturity of the of the of the customer.

0:26:49.300 --> 0:26:49.840  
Interviewer  
Umm.

0:26:49.960 --> 0:26:54.440  
UPR4  
But from a vulnerability perspective, it…it normally comes down to something. That's that's pretty. That's pretty simple, you know it. It's it's normally out of date systems and software. You know where they've just not they've just…The…the…the budget isn't there or the forward planning isn't there to uh to to implement new systems because you know, if you've if you've got a load of applications on on some old servers and they only run on that old set it it becomes a big piece of work to do. Uh at that and so…And I think they said before is kind of the awareness aspect of it. You know, companies that that run without any and…and I understand for smaller companies can't afford it. But for larger companies, they don't have anybody responsible for security. They might have somebody who's accountable for data protection, but that person's not responsible for security aspects of it. It's normally the IT manager. So then you've got you've got a conflict of interest because the IT manager wants to make sure things work. The security person wants to make sure things work securely and it's…it's a different mindset so.

0:28:14.110 --> 0:28:22.180  
Interviewer  
Then a question numbers six I think I'm going to change a little bit because you are more like doing like the…the prevent. So you said you for the maybe for the incident response you work with some maybe some partners. So when your customers they encounter this incident. So in terms of the…the mechanism, the mechanism for harm reduction and incident management, what would you suggest for your customers to do?

0:28:46.530 --> 0:29:7.780  
UPR4  
Uh, normally we what we would do is we would put some sort of instant response plan together to…to…to enable them to run through the…the…the process, whatever that process has depending you know as it could be isolate it depends…depends on the client as well and depends on the criticality and depends on the incident. It's one of those sort of things.

0:29:11.480 --> 0:29:11.940  
Interviewer  
OK.

0:29:13.760 --> 0:29:16.750  
Interviewer  
And then let's go to question number seven. So I want to ask that and how do you describe the cyber resilience of your most of the customers?

0:29:28.990 --> 0:29:29.780  
UPR4  
For most of the customer...So what we trying to do is anything that we do, we…we try and make sure it's tied back to an international standard or…or guidance.

0:29:38.590 --> 0:30:0.410  
UPR4  
So you know any, if we're asked to implement for something really, really simple, an access control policy would make sure that it's written with ISO 27001 in mind, with the control stated in that. If we're looking to…if we're doing penetration testing depends on what it is. So we…we look at OWASP or we'd look at CIS benchmarks. So from a so we will always do…Anything we do is backed up by good practice or the NCSC practice. So I would say that what we do meets the…the necessary standards.

0:30:25.760 --> 0:30:31.30  
Interviewer  
And then question number 8 is among of services you provide, in what aspect do you want to…uh, do you think it's still insufficient? And maybe in the future we want to improve.

0:30:41.710 --> 0:30:42.220  
UPR4  
Yeah.

0:30:42.230 --> 0:30:50.10  
UPR4  
OK, so I just said we've just started to provide a software and services. So our managed qualis. So I'd like to expand out to provide the more 360 degree view of cyber enforcing technology. So for instance, antivirus maybe some form of Active Directory security gate controls, so we'll look at so I could look at all so I could actually go into a company and provide them a whole suite of technology that would help them meet their cybersecurity goals.

0:31:28.480 --> 0:31:29.720  
Interviewer  
Yes, I think it's. Yeah, you've already answered question number 8, 9, 10 cause it's kind of like a related question.

0:31:39.300 --> 0:31:39.500  
UPR4  
Yeah.

0:31:39.230 --> 0:31:46.660  
Interviewer  
So that's go to Section G, so section G is like the question about public private partnerships.

0:31:47.90 --> 0:31:58.250  
Interviewer  
So the first question is in terms of the uh, public private partnerships in the cybersecurity, uh, what do you think about this idea? Does that really help?

0:32:0.760 --> 0:32:1.730  
UPR4  
Yeah, I think it's. I think it's really important. I have to draw, certainly industry and…and government together in cybersecurity because, uh, the…the government is would not be able to govern without an economy and the economy's made up of private companies and…and…and vice versa.

0:32:25.490 --> 0:32:29.280  
UPR4  
And also government gets a wider viewpoint on what's going on than…than…than then private companies. Certainly. Certainly we, then…then errors are most…most companies. So yeah, I think it's a I think it's a real help in this thing. It's a really important thing to do.

0:32:48.130 --> 0:32:55.260  
Interviewer  
And then so in terms of the this cooperation, what do you think that the public sector can contribute to this partnership and also from the private sector. What can they contribute to?

0:33:4.510 --> 0:33:11.90  
UPR4  
OK, so so the from the public sector, so the NCSC, which is obviously the UK's body, they contribute. At the moment, you know it's certainly contribute on good practice. They will inform of any up and coming threat alerts, so they provide that the same with the Nazi and America and they'll provide you with sort of educational pieces that did, you know for different for large companies, small companies, individuals, etcetera.

0:33:38.690 --> 0:33:41.550  
UPR4  
So I think that's…that's really good from that perspective.

0:33:42.940 --> 0:33:52.540  
UPR4  
They've also got cyber whatever information sharing partnership they were a member of CISP where they have. You can join that and you get more information there, but there'll also put interest groups together. So, for instance, if you're if, if, if you specialize in maritime, they'll have a group about maritime, which you'll have other stakeholders who are maritime related as well, and security so you can get an idea of what's going on in your sector. So I think that's certainly government or public sector can provide. There's probably more uh, I think.

0:34:28.690 --> 0:34:33.200  
UPR4  
I I think from a private sector perspective, it's probably the innovation side of things. You know in this you know, because we can, we can be more agile and we're not sort of as bound by bureaucracy. So I think certainly a lot of the tech providers, you know from a cybersecurity perspective can bolster cybersecurity because certainly you know some of the…the…the threat monitoring companies can…can input into the…the UK cyber response units etcetera, and I know they do anyway. So…So that's I think that's a good idea.

0:35:9.330 --> 0:35:11.580  
Interviewer  
Then let's go to question number 2. And so I'll see you now. Uh, do you know the current pri…the public private sector cooperation mechanism.

0:35:20.350 --> 0:35:21.960  
UPR4  
A general idea? Yes, that's so said we've got the the NCSC.

0:35:25.250 --> 0:35:33.560  
UPR4  
Obviously they they provide webinars and you have like UK cyber which is a an annual conference.

0:35:34.170 --> 0:35:42.180  
UPR4  
You've got CISP, which is the Cyber Sharing partnership, and I think NCSC have just started a new something cyber 100 (Industry 100)…I can't quite remember the name, but…where you can go and volunteer to work with the NCSC you or your company can volunteer you. So you…you give them a day, a month or something to further enhance those ties, I think, yeah, I think they're good idea. I think yeah, it helps. It helps the NCSC understand what goes on in, in, in industry and…and vice versa.

0:36:12.940 --> 0:36:13.790  
Interviewer  
OK.

0:36:13.920 --> 0:36:20.310  
Interviewer  
And then so how do you evaluate this kind of partnerships?

0:36:23.110 --> 0:36:23.740  
UPR4  
OK. I yeah, I think I think they're a good idea. Whether there's…there's room I think in in some ways the NCSC probably needs to go to advertise them more and…and, you know, improve visibility. Uh, I think the other problem is that small companies can't really afford time to put people into these sorts of schemes that the…the cyber 100 (Industry 100), so they end up getting only the larger companies are able to afford that. So, therefore they get greater benefit from it. So I think that that's that's part of part of a an engagement problem really from that perspective.

0:37:17.50 --> 0:37:18.110  
UPR4  
So I think they could be improved. I don't know how that could be improved, unless NCSC paid for it. But so unlikely.

0:37:26.320 --> 0:37:33.920  
Interviewer  
OK, so most of it is engagement problem?

0:37:31.170 --> 0:37:32.800  
UPR4  
Yeah, I think so, yeah.

0:37:33.930 --> 0:37:37.800  
Interviewer  
So in addition to add umm, so do you…Umm. What difficult…What difficulties do you think that that will be when this partnerships are, you know, happening?

0:37:50.540 --> 0:37:59.70  
UPR4  
And it was, I think you know, these partnerships are happening and I think the…the difficulty is…is getting engagement from smaller businesses. I think you…you tend to find it's the larger businesses that…Engage more because they can afford to. You know they can. They can send somebody off for, you know, a on a free trip to go to spend a day in London to talk about stuff, whereas you know, smaller companies like ours and others would have that be a day that somebody wouldn't be earning any money. Uh, and I think that gives a...It means that the…the larger consultancies get closer to government, whereas the smaller ones get pushed away. So I think that's…that's an issue and doesn't really meet with the UK's small and SME agenda for business. Never mind cybersecurity.

0:38:44.700 --> 0:38:50.180  
Interviewer  
And then in your opinion, what do you think that could be done to…Uh, and make those small business to engage more in this cooperations?

0:39:2.340 --> 0:39:4.220  
UPR4  
Uh, yeah, so so an interest. It's an interesting one because it comes down to…to time and funding and…and small businesses have…have neither. So you…you probably have to look at some sort of streamlined way of meeting whether the leverage go back to you know more teams calls zoom type calls, uh, maybe, maybe set up a specific small business working group. You know that that can and get the voice of the small business heard or the…the…the more niche businesses heard that might be that might be an idea.

0:39:44.250 --> 0:39:51.690  
Interviewer  
OK, so you said it is about the budget constrained. It's because of the…the money they…they need more. They need to put more money to invest and also they need more incentive to cooperate, OK.

0:40:6.420 --> 0:40:7.360  
UPR4  
Yeah, I think so.

0:40:10.300 --> 0:40:17.360  
Interviewer  
OK then umm, so I'm going to and go to question number 5.

0:40:17.530 --> 0:40:24.80  
Interviewer  
So in your experience, do you have any this kind of partnerships?

0:40:25.550 --> 0:40:26.40  
UPR4  
Yeah. So so as a NCSC assured cybersecurity consultancy we and we go up to NCSC, I think as at once a month or or, you know to spend spend a day with them and they then tell us about their initiatives and and and all that sort of stuff. Yeah.

0:40:43.740 --> 0:40:44.850  
Interviewer  
Umm, OK.

0:40:44.860 --> 0:40:54.120  
Interviewer  
And so in this partnerships, umm, in the future, what do you want to move forward to maybe to improve this partnership?

0:40:58.60 --> 0:40:58.780  
UPR4  
OK. Uh, probably…better information sharing.

0:41:7.350 --> 0:41:26.700  
UPR4  
Also from…as a as a wider piece is the…the probably the fact that government procurement is…is weighted against the smaller consultancy and…and…and so if they want us to help make the UK safer place, they need to…they need to enable us to be able to help instead of just the larger consultancies.

0:41:38.600 --> 0:41:41.10  
UPR4  
When I see a large, I'm talking very large.

0:41:41.940 --> 0:41:51.830  
UPR4  
Yeah, you know, I you know, so we end up having to supply people into them, whereas if the government went to us directly, they get us cheaper than what they're paying for these larger. So I probably just have a greater understanding of or a greater appreciation of their skills.

0:41:59.560 --> 0:42:0.90  
Interviewer  
OK.

0:42:0.840 --> 0:42:10.750  
Interviewer  
Can you talk about more about about information sharing because the information sharing, umm, do you think it's balanced? From the public uh also from the private sectors.

0:42:17.980 --> 0:42:25.980  
UPR4  
I…it so, I mean I've…I've worked in in the environments where we don't share, so I know it's not balanced. So, uh, so from a public to private. So no, it's not, but it…it depends on what…what you need people to…to know. Uh, you know? So if if it comes down to…uh patching or or or or specific vulnerabilities in systems etcetera that that that should be declared straight away and not not kept to to kind of facilitate and intelligence gathering operations. Let's put it that way.

0:43:13.30 --> 0:43:15.350  
Interviewer  
And then so for the information sharing. What could be shared more in the future from the public sector, and from the private sectors?

0:43:26.910 --> 0:43:27.600  
UPR4  
And.

0:43:35.110 --> 0:43:35.870  
Interviewer  
Umm OK.

0:43:29.820 --> 0:43:36.590  
UPR4  
I don't I, to be perfectly honest without knowing what that information that they hold that wouldn't be able to tell you it's a it's a, you know? And and unless you…Yeah, I couldn't tell you what they could, what they could share.

0:43:41.370 --> 0:43:41.820  
Interviewer  
OK. I understand.

0:43:43.70 --> 0:43:44.320  
Interviewer  
So like in what aspect? Because maybe some of some of the the general public they maybe think that…umm, not not. Sorry, not the general public. Some private companies, they think it's always there they to share to the government, but they think the government, they don't really share enough information to them. So they don't know how to do it. Do you encounter these kind of difficulties or?

0:44:13.570 --> 0:44:14.780  
UPR4  
No, not in, not in what we do so no.

0:44:17.230 --> 0:44:23.680  
UPR4  
So we we don't encounter anything like that because we we're we're we deliver consultancy and penetration testing. I think I'd be more on the threat analysis and intelligence side.

0:44:29.40 --> 0:44:29.460  
Interviewer  
OK. Yeah, I think that's enough.

0:44:35.810 --> 0:44:36.170  
UPR4  
You sure?

0:44:35.260 --> 0:44:37.290  
Interviewer  
Yeah, I think that's, yeah. Yeah.

0:44:37.300 --> 0:44:37.610  
Interviewer  
Yeah.

0:44:38.60 --> 0:44:45.20  
Interviewer  
And or OK, I actually want to ask more about about awareness. So can you tell me more about the and how do you how do think about uh and how how sorry, how do you evaluate the public…general publics awareness on cybersecurity?

0:45:0.660 --> 0:45:2.130  
UPR4  
Uh, OK. So I think there's a lot of information out there about you, you know, cybersecurity. But I think people have gone a lot of people kind of blind to it. They've they've seen it so much. You know the company X has been hacked and because, oh, that's a shame. And then you know, then and then they go. Yeah. So what? you know? So I think there's a I think there's a lot of information out there.

0:45:29.320 --> 0:45:34.710  
UPR4  
I think there's a lot that's not just cybersecurity, it's privacy related as well, because it's people's privacy. But I think the general public, as a whole fundamentally don't really care. You know, I mean, I talked to businessmen and companies and, you know, and a lot of them, it's all about making sure they're making enough money. It's not about making sure there's secure unless the government actually mandates that they have to meet a certain level from cybersecurity. They, they, they, they will not do it or they will do it only because one of their larger clients tell them they have to. So.

0:46:12.80 --> 0:46:14.180  
Interviewer  
OK and. So the…when they don't want to do it unless the clients tell them to do it, or maybe the policy.

0:46:27.610 --> 0:46:28.210  
UPR4  
Policy. Yeah.

0:46:27.610 --> 0:46:29.380  
Interviewer  
Uh, when the when the policy?

0:46:29.110 --> 0:46:36.790  
UPR4  
Yeah, so so you know, for instance, we we get we get calls with, I'll just give an example.

0:46:37.40 --> 0:46:43.790  
UPR4  
You know a software company and that does stuff for Tesco's, the supermarket, Yeah? You know, and but Tesco's will will give this small company a questionnaire about cybersecurity, you know? Is everything encrypted? Do you have an access control policy? Do you have firewalls? Do you have XYZ and they don't have any of it, but they don't really want it, but they know they have to get it because Tesco's said it shouldn't be Tesco's, saying it should be the government. Yeah.

0:47:10.620 --> 0:47:12.240  
Interviewer  
OK, OK.

0:47:21.790 --> 0:47:21.970  
UPR4  
Yeah.

0:47:13.150 --> 0:47:23.220  
Interviewer  
So I think that that's the that's the good part of partnership because the the government, they have the power to tell people to do it. To tell the the the private sectors.

0:47:34.500 --> 0:47:34.660  
UPR4  
Yeah.

0:47:26.490 --> 0:47:36.740  
Interviewer  
You have to have this this kind of regulations or you need to reach this this standard so you can have a good cybersecurity, OK.

0:47:38.480 --> 0:47:51.840  
UPR4  
Yeah, so so they have, they have started in public sector where you have to reach the standard of cyber essentials, but Cyber Essentials is…is self-assessed. Cyber Essentials Plus is externally assessed. So and so and we've gone into companies before, who are Cyber Essentials. And we've had to basically tell them to start again because they've not…When you have known security people answering security questions, they will answer the question. So they pass the exam, not necessarily implement the controls as said. Yeah. So that's so self-assured schemes. They're OK, but they're not actually, they're not assured. They're not. There's no guarantee of quality or…or control so.

0:48:37.820 --> 0:48:40.750  
Interviewer  
Umm OK quality.

0:48:44.460 --> 0:48:45.130  
Interviewer  
OK.

0:48:45.140 --> 0:48:47.630  
Interviewer  
Yeah, I think that's, umm, that's it?

0:48:47.960 --> 0:48:51.10  
Interviewer  
Yeah, I got a lot of information from you.

0:48:51.240 --> 0:48:51.640  
Interviewer  
Yep.

0:48:53.40 --> 0:48:53.380  
UPR4  
Good.