**Interviewer** 0:09  
And also there will be.  
Transcription on the site. Yeah.

**UPR5** 0:14  
OK.

**Interviewer** 0:15  
So it is hard for me too to do the the transcription later, so then then should we should we start? Because yeah, we only have one hour and.  
And OK, so that's got started and let's start from section A.  
Section A is for the basic information, so for me for the first question I would put you in private cybersecurity providers. I know you are the founder of the [the name of a company] and I yeah I googled it a bit and yeah, it's a it's amazing the thing that you do so I would, yeah.

**UPR5** 0:53  
Ohh thanks.

**Interviewer** 0:55  
And I would like you to, can you tell me more about this…[the name of a company] and what's…what's your responsibilities and what position you are the founder. So yeah, tell me more about that.

**UPR5** 1:10  
Yeah. I'm the founder and the day to day director, managing director.

**Interviewer** 1:15  
Mm-hmm.

**UPR5** 1:15  
We have very small actually, but we have some very respected in people.  
We've been working for 22 years now in this space. And we have some quite, I would say, quite impressive client for cyber small organisation across government and private sector from some of the major departments and also major financial services organisations. And we've worked for, you know, places companies like [the name of a company], [the name of a company] and…and so forth. So, so…so it's always been from my house. OK, I never had a office been working from my house for 22 years and my..my colleagues worked from their houses so it's very virtual, very digital setup.

**Interviewer** 2:02  
OK. Umm. OK, so uh, then that's uh, jump to section E. Yeah, because I think the BCD, it's, yeah, it there for the…the police.

**UPR5** 2:22  
Yeah, I I can't actually open it, by the way. So I don't know about the attachment is.  
I think it's my problem here. I have some technical problem and it's a fix, but I notice I can't open the PDF and Teams isn't working. So I need to I need to do some checking.

**Interviewer** 2:37  
OK, it's OK. I will….I mean, I will…um…ask you the question again. So yeah, you can.  
So section E is for…they are all for the cybersecurity question and more comprehensive question. So for the first question is what are the major cyber attacks in the UK like, as you know, and what are the modus operandi and can you also give me some examples?

**UPR5** 3:06  
OK, I think maybe it's happening now. I restarted my my yeah, I've I've got it now.  
OK, I restarted my. I'll click on that fixed the problem.  
So section E major attacks. OK so. First of all, it…it depends on the sector. OK, so for example in financial services, we can think about Ohm's attacks on the financial organisation itself and a tax on the customers of the organisation because both of these are concerns for the organisation's, OK.

So in terms of attacks on the organisation, the most common scenarios would be ransomware. So, as you know, this is, let me I don't I want I will tell you the details if you ask me.

**Interviewer** 3:55  
OK, I know ransomware.

**UPR5** 3:56  
So, ransomware, data breaches. And. So something sent spyware for, again for data theft, but it's not a…it's not like a database attack, right? So database attack, they take the whole database. Spyware, maybe they watch the keyboard, or they watch the camera or the microphone, and denial of service attacks on the web service. OK, so I would say those are the four top issues now.

**Interviewer** 4:26  
Umm.

**UPR5** 4:31  
I'm not basing this on any sort of statistical survey. You'll get surveys with different results if you look at them, but just based on my experience with my customers, yeah.

**Interviewer** 4:40  
Umm. OK, so that that's perfect.

**UPR5** 4:41  
Yeah, I'm with my students who are police officers.

**Interviewer** 4:45  
OK.

**UPR5** 4:46  
So that's why I was saying that's the main threat, set of threats at the moment.  
Now there's a new threat vector that is evolving which of course, is generative AI.

**Interviewer** 4:57  
Generative AI, yes.

**UPR5** 4:59  
Yeah, but we don't know what the issues are going to be. We have some early indications, but I can't say that it's a major threat. It's…it's a…it's a major threat because it's potential. OK. But it's not a major risk right now because there's no statistical data. OK. So risk, like frequency and impact risk, because risk, so you need to know the frequency and the impact to know if it's a risk. So, but it's definitely a threat. And in the in that space for financial services, I would say the main issue would…would be at least for financial services organisation, the issue would be employees using it without permission in, in, in ways that involves them. For example, uploading some data saying to take things to AI. I have this report. Please give me a better version. I have this software code. Please…please check it for errors. Things that are giving away information to the AI tool. So that, disclosure of information.

**Interviewer** 5:59  
Umm.

**UPR5** 6:01  
OK. So that's the organisation then the customers of the organisation. OK, so…so generative AI is definitely an issue for customers because it can be used. It's…it's like you. You combine it right? So you do your online search to…to find the target your criminal, right? to…to find the target, and then you do your AI based attack to create fake image. Create fake LinkedIn page, fake website, fake email. So it's marrying the AI to the existing traditional search to find mixings and being more sophisticated in your romance fraud, identity theft. Uh. Other frauds to extract payment in details from people, phishing or even investment fraud. OK, so you're pretending that you have an amazing new opportunity for them to invest money that type of fraud. So even proper…, you could even imagine some, probably, I don't know if it happened yet, but some property scams where you have amazing photographs, looks like amazing house in an amazing place with people, happy people. But it's not the place doesn't even exist on the planet. OK.

**Interviewer** 7:18  
Ummm..

**UPR5** 7:18  
It's just the AI image. So…so all these things are coming somewhat happening. Some are probably going to happen soon. I think that's a big risk area. Apart from that, some of the traditional phishing attacks and social engineering attacks are…are very common and also. So when there's a data breach somewhere, it doesn't necessarily have to be a data breach in the banking system. It could be a data breach on Netflix or…or even some small membership organisation, but the data that is there can be the same data as the banking data.

**Interviewer** 7:53  
Mm-hmm.

**UPR5** 7:53  
For example, credit card CVV 2 pin, date of birth, email address, these things, and then that gets used for financial crime against the banks customers. So a card not present fraud, for example, are you familiar with this?

**Interviewer** 8:03  
Umm. Yes, yes, kind of.

**UPR5** 8:10  
OK. Yeah. So it's very messy. OK, it's very messy. The data is stolen here. That's a crime, but the data is used over here to target the customer. That's another crime, you know? So it's quite complicated.

**Interviewer** 8:23  
Umm OK, I understand that. Yeah. This really. Yeah. Thank you for umm a lot of information about that. Yeah. Then let's go ahead to the second question. So now we know, umm, about the…the major cyberattacks in the UK and what are the major targets of cyberattacks in UK and also what are the reasons?

**UPR5** 8:48  
OK. So they're different targets for different reasons, obviously, so obvious. So people, as I mentioned, mainly it's the financial motive. And so, well, OK, so there is the acquisitive crime, OK, crime where you want to make some money or take something from somebody that's…that's targeting the people finance…for financial reasons.

**Interviewer** 8:57  
Mm-hmm. Umm.

**UPR5** 9:10  
But there, there's quite a lot of things happening around misinformation. Umm.  
And the use of fake accounts to spread misinformation through news feeds, social media, you know, YouTube and so on., Tik ToK, Instagram, and this is…this is also a class of criminal activity because you're creating a false persona and telling mistruths with a with a malicious intention, OK?

**Interviewer** 9:36  
Umm.

**UPR5** 9:38  
So, and I would say that's very, very important right now, particularly given the conflict that is happening around the world today. So. So that's a big issue, doesn't get a lot of attention all the time, but it's a big issue. So that's one. OK, that's targeting people. And romance fraud is included in that social engineering.  
When I say social engineering, I mean romance, fraud, investment fraud.  
All of these things, they're under their heading of social engineering, OK.

**Interviewer** 10:07  
OK.

**UPR5** 10:11  
OK. So in terms of organisations, so we talked about financial services earlier that it's on that list that and I already talked about the reasons which I make mostly either data theft or financial crime.

**Interviewer** 10:18  
Umm.

**UPR5** 10:26  
But other organisations include our critical national infrastructure. So, you know, electricity, water, communications, that medical OK. And very often the motive there is not financial, it's strategic conflicts, strategic military or ideological motivations.

**Interviewer** 10:47  
Mm-hmm.

**UPR5** 10:49  
And then finally, we have the…the…just the…just the business sector in general, OK, it can be competition. There have been cases of attacks taking place because a competitor wants to stop this business from operating. So some denial of service attack. It can be state sponsored because by targeting an important sector in the economy, even if it's not critical national infrastructure, you can cause harm. Intellectual property theft and, of course, blackmail or ransoms. OK, so there's ransomware, which is the software malware, but you can also ask for ransoms. You know, you can do a denial of service attack and say if you don't pay us, we'll do it again. OK, so there are other ways to take ransoms.

**Interviewer** 11:37  
And.

**UPR5** 11:38  
So so generating ransoms normally in cryptocurrency, normally in Bitcoin or Monero um, that's a big motive. I hope I'm answering your question.  
So. So the size I break the major targets into those four groups. People, critical national infrastructure, financial services as a separate public because it's so big. And then other organisations.

**Interviewer** 12:02  
OK, so people and people and some critical national infrastructure? OK.

**UPR5** 12:07  
People, critical national infrastructure and then financial services. People will say, OK, financial Services is part of critical national infrastructure, but it's such a big one and it's so unique that I usually break it out and then other organisations, you know, people attack Tesco, you know, people attack, telephone, selling, sales, outlets. So…so it could be any one of those.

**Interviewer** 12:34  
OK. Thank you so much. Then I want to ask something more like…um… Are they any specifics industry that are more easily than other industry to become the target?

**UPR5** 12:48  
So industries that are…are critical but not high tech.

**Interviewer** 12:54  
Hmm, not high tech, OK.

**UPR5** 12:55  
OK, not high tech, so high tech sectors that tend to have a good level of cybercrime awareness, cybersecurity awareness. Sometimes it goes wrong, but normally you know if it's a high tech organisation, they will understand the issues and they're usually OK in most scenarios, right?

**Interviewer** 13:11  
Hmm hmm.

**UPR5** 13:12  
But if you take something like water supply. OK. Yeah, it's not.  
It's not a high tech space, but it's critical.

**Interviewer** 13:21  
Hmm, sounds like manufacturer industry?

**UPR5** 13:23  
No, no. Like providing water to the house.

**Interviewer** 13:30  
OK, OK.

**UPR5** 13:30  
Yeah.Yeah. So for just bringing water to the house and the pipe, OK.

**Interviewer** 13:35  
Umm.

**UPR5** 13:37  
No, in the UK, I don't think we had any problems yet, but in the US they definitely had some cases that we're not 100% sure was it an attack or was it a mistake?  
But there have been some cases where water supply has been interrupted by…by cyber means OK or they added chemicals to the water through the cyberattack.

**Interviewer** 13:51  
Umm. Umm. Ohh.

**UPR5** 13:58  
Yet I think I can't remember the name of the place now, but there was a large case a couple years ago, so that's the concern for me because water supply, even electricity, you know, is the electric company really, you know, top level cyber secure. I…I don't think so. But you know, I…I doubt it. I don't know. I haven't been there, but I…I…I…I'm suspicious about that. OK, so I think those…those are…those are places particularly at risk. There was the critical service, but not a high tech mindset, with the high tech skills that.

**Interviewer** 14:35  
OK, critical, but not high tech, OK.

**UPR5** 14:40  
Yeah. Think, for example trucking. So so you know, if you look at the roads in the UK, everything's in the trucks, right? Everything…

**Interviewer** 14:45  
Ah, trucking. Yeah, yeah.

**UPR5** 14:47  
Are these companies high tech? Do they have, you know, good cybersecurity around their management for their trucks…and uh, the fleet management, things like this and you could cause a lot of chaos with those organisations targeting.

**Interviewer** 15:03  
OK, then let's go to uh, question number 3. So then what are the factors affecting the cybersecurity in the UK?

**UPR5** 15:16  
OK, I think so. The main factor…the main dependency is awareness.

**Interviewer** 15:23  
Awareness, yeah.

**UPR5** 15:23  
OK. Always, umm. We talk about the human firewall. Maybe you heard this phrase before. OK, so humans are the first line of defence. Because normally even the most complicated, you know, state level attacks, they often start with an email, somebody click a link, and somebody posted their password online. Even the top level attacks stuff like this. So human…human awareness is key education, training, and possibly, you know. It's it…it's already there at school, but maybe not sufficiently in depth at school.

**Interviewer** 16:01  
Umm.

**UPR5** 16:01  
OK, kids are very technical these days. They can understand it, but we need to tell them more. So that's the first thing. The second is…the age of some of the infrastructure.

**Interviewer** 16:15  
Umm.

**UPR5** 16:15  
So in the industrial spaces and in places like power and water and so on, very often the ohm, the, the IT infrastructure, particularly the management systems like they call them SCADA Systems, SCADA, yeah. They can be 25 years old sometimes

**Interviewer** 16:31  
SCADA.

**UPR5** 16:35  
Sometimes it's like quite a high percentage, uh, 25 years old. And they've been attacked in the past. In others, for example in the stocks net attacking Iran, it was the SCADA system that they targeted.

**Interviewer** 16:51  
Mm-hmm.

**UPR5** 16:51  
And if you look around the industrial plant in, in the UK and Europe and the US, it's quite old. So, so there's some risks there.

**Interviewer** 16:57  
Mm-hmm.

**UPR5** 17:04  
Factors. OK, so the…the rapid change of technology. OK. So smart devices. So not generative AI, but the AI in the AI enabled devices, smart devices. They turned the house and the office into a much more digital place than it was before.

**Interviewer** 17:27  
Umm.

**UPR5** 17:28  
And so every…every digital device that you add to your house, it's another risk.  
OK, so…so we don't really think about it. You know, we just go my office now. I'm in my house, right? I have like 1,2,3,4 digital device just in this room. OK, then I have more than the other room and more in the kitchen.

**Interviewer** 17:45  
Umm.

**UPR5** 17:48  
And you know, every time we add one, I have, my car is connected to Internet. So every time we add one of these devices, the risk is increased, but we don't really think about that. So digitization of the…the home and the workplace with smart devices, I think. It's Internet of Things. It's a big it's a big area of risk up, mostly because there's no global standard for manufacturing and security of these devices.

**Interviewer** 18:12  
Umm.

**UPR5** 18:14  
So you can have a small factory somewhere and make any digital device you choose, put it on Amazon and next thing it's in people's houses in in many countries.

**Interviewer** 18:29  
OK. Yeah, that's a lot. And had about the for example like um…political issue or geopolitical issue, yes?

**UPR5** 18:37  
OK. Yeah. So that's another dimension of the propaganda dimension. So I have mixed feelings about this because propaganda is not new, right?

**Interviewer** 18:44  
Umm.

**UPR5** 18:44  
And it was equally effective if you go back to 1939, you know, World War Two beginning the propaganda was equally effective.

**Interviewer** 18:52  
Umm.

**UPR5** 18:54  
The society was equally divided as it is now. Umm, they were reading it in the newspaper. They were reading it on the leaflets. They were listening to people speaking in the public spaces. OK, it was very, very contentious and there were many people here in the UK supporting the Nazi party in a in America, there are many people supporting the Nazi Party in 1939. So I'm not sure it's actually changed that much with the digital activity.

**Interviewer** 19:21  
Hmm.

**UPR5** 19:22  
It's just that we…we can all see it and feel it, you know. So I have mixed feelings, but it's definitely an issue. There's definitely a problem with the disinformation and the influencing of public opinion through various channels, but I, as I say, I think it's always been like this.

**Interviewer** 19:36  
Umm. Umm.

**UPR5** 19:44  
My main concerns digitally for the general society would be the impact if we lost the communications, the telecom and data communications networks, OK. So if you look at the, have you ever looked at the global cable map?

**Interviewer** 20:04  
No.

**UPR5** 20:05  
OK, have a look at the global cable map.  
It shows you all the cables for…for Internet and phone on the planet.

**Interviewer** 20:11  
Umm OK.

**UPR5** 20:14  
And they have…. That they're…that it's like they…they all feed into UK in one place, you know, and they…they feed into the into Japan and the one…one place and there's about three or four different locations on the planet where all the cables are very concentrated. And literally if you had a nuclear disaster or even an attack at any point just one or two places, the whole network would…would be down for the whole planet, for the whole planet.

**Interviewer** 20:20  
Umm.  
Hmm hmm.

**UPR5** 20:42  
So that's my…that's actually my main concern or…or…or a huge cyberattack.

**Interviewer** 20:48  
Cyberattack OK.

**UPR5** 20:48  
Yeah. Yeah, but more likely…OK…a nuclear attack on the cyber on the cyber infrastructure.

**Interviewer** 20:57  
Hmm, yeah, that would be a huge problem.  
Like especially.

**UPR5** 21:00  
Yeah.

**Interviewer** 21:01  
You have you used that kind of technology to like file a nuclear war and also you can really…manipulate people’s thoughts and opinions about that and then you will be…

**UPR5** 21:14  
Yes, yes. Yeah. Yeah. And do you remember when the Ukraine Russian conflict, the most recent conflict started? They had the Nord stream pipeline in the Baltic. It was destroyed by an explosion. Do you remember this got pipeline?

**Interviewer** 21:28  
Oh, yeah. Yeah. Yeah. Yeah, that's uh huh.

**UPR5** 21:30  
Yeah. So exactly the same, exactly the same thing could happen to the Internet cables, and then we would lose banking, communications, governance, defence, communications, and transport food supply, everything.

**Interviewer** 21:45  
Hmm. OK, then let's go to section F. So section section F is more like the cyber defence strategy that for the cybersecurity firm. But let me see if some of the questions are…they fit for your situation. So I think the first one is, yeah, what techniques and services that you provide to your customers in the field of cybersecurity?

**UPR5** 22:13  
OK. So we provide so training for non-technical staff who need to understand the threats. And we also provide some skills training on Internet searching. So yeah, well are called Ostend. Yeah.

**Interviewer** 22:31  
OK, so more like training and training to.

**UPR5** 22:36  
Yes, yes.  
So we used to be consulting, but I haven't done any consulting for maybe 5-6 years now is it's…it's been everything training. So classroom training and also e-learning development.

**Interviewer** 22:42  
Hmm. OK, trying to e-learning.

**UPR5** 22:50  
Yeah.

**Interviewer** 22:50  
OK.  
Then, because I am your LinkedIn profile says that you…you also deliver the solution for corporate and…and governments. But you said it was like 5 years ago, so now you don't do that anymore?

**UPR5** 23:06  
Yeah, I need to look at my profile again, but yeah, I haven't done that. I mean, I will do it if they ask me, OK? In fact, in fact, I'm doing a bid right now for some consulting work, so sometimes we do consulting work, but I try…I'm trying not to travel too much, so for me the training is perfect, so I've been focusing on that, but I still do some consultancy.

**Interviewer** 23:25  
Umm. Hmm. OK, then let's go…then number 2…number 2 and who are your major customers?

**UPR5** 23:35  
Yeah. So this one, uh, unfortunately I can't name the customers. I can tell you the segments, the segments that they're in, like which part of the economy they are in, but I can't name the customers because of confidentiality, but…but we have we work in banking sector, we work in policing. We do some work in just the general government. That's yeah. So those…those…those are the three main ones for us.  
We previously we did a lot of work in shipping, maritime transport, but I haven't done that for a few years.

**Interviewer** 24:16  
OK. So when you said banking, policing and general governments, were you talking about the training and e-learning?

**UPR5** 24:24  
Training and learning and consulting…when…when even.

**Interviewer** 24:26  
And consulting and also OK and consulting.

**UPR5** 24:27  
Yeah, yeah, yeah.

**Interviewer** 24:29  
OK. And then question number 3. When they when they go, go to seek for your help, what are the…the major reason? Like what are…the major reason that make them to come to you for help?

**UPR5** 24:44  
Yeah. OK, so I think. It falls into a couple of categories, so a lot of our business is repeat business, OK. So we have customers and we managed to keep them for 10 even 20 years, sometimes. OK, so keeping the customer happy. Always providing the best quality that you can provide. Very important, right? Being we're competitive on price, but we're not cheap, you know? But…but we you know, we…we will compete. New customers often come towards because they heard about it through another customer. The word of mouth. OK, sometimes it's their competition and they…they ask what…are these guys good doing or they're using [the name of a company] for this. Maybe we should use them also, right? So I had such a call just now actually that one hour before. Right.

**Interviewer** 25:39  
OK.

**UPR5** 25:40  
Other times, because very often what you find is that, say the manager in company A who is using us and likes us, leaves the job and goes to Company B, and the first, you know, the first phone call. Can you help me in this company? I had one guy like that. He's moved three times, OK, and each time he moves, the calls me. So then I have that relationship with that company even when he leaves the other one, I don't lose that relationship. I keep it and then I get a new relationship also.

**Interviewer** 26:13  
Umm, OK, that's really nice. It means that you are like they…they are really happy about your services and…

**UPR5** 26:19  
This is the main thing. If you want to run a successful business, make sure your customers happy. That's the most important thing.

**Interviewer** 26:25  
Hmm. OK, then let's go to uh, question number 4. So among your customers, what do you…what…in what…what aspect do you think they are insufficient the most? Of course, in terms of cybersecurity.

**UPR5** 26:43  
Yes. Yeah. I think it's going to come back to the awareness, I think…uh, when you have the people in the room, and you're talking to them. They OK then then…It's an issue, but they don't understand it.

**Interviewer** 26:56  
Hmm.

**UPR5** 26:57  
OK, so they're…they're happy to learn, right? They…they know there's a problem, so it's not like you have a situation where ohh there's no problem here, but they know there's a problem but they don't understand that problem. So they actually want to hear and they want to learn. So it's quite easy to communicate with them. But yeah, that lack of and it's because of the subject. It's a technical subject that most people are not technical. Some people are really scared of technology. As soon as you say the word, you know digital. They are like…oh, I don't know.

**Interviewer** 27:24  
Umm.

**UPR5** 27:24  
Yeah. So. So so there's a fear. And because…it's because they are afraid, they don't go and learn or teach themselves, OK, if it was about football or something, they would learn by themselves. There's no way I can't make any money selling, you know, football information. But yeah, once you say digital, they're very afraid. And you have an opportunity to sell them the training.

**Interviewer** 27:46  
Hmm. OK. And how about if, like most of your customers, are they, umm, not from your customers…like in your experiences…like, do people…are people willing to put more money into this cyber…to strengthen their security?

**UPR5** 28:10  
So that's really interesting. Very often they're not willing until another organisation in the same space, same sector gets hit.

**Interviewer** 28:20  
Gets hit OK.

**UPR5** 28:21  
Yeah. So like the hotels for example and then not going to spend anything on cybersecurity and then the Marriott gets hit big time and every hotel in the world in the planet is spending money on cybersecurity.

**Interviewer** 28:27  
Hmm.  
Hmm, OK.

**UPR5** 28:31  
Right.  
But then there's slow down. Then for, you know , the cyber thefts they forgot, and now the systems are going, you know, and then they get hit, someone gets hit and everybody spends money. Actually I…I made a case to say, you know, the cost of cybersecurity around the world. The real cost is not the cost of the…the hack or the cost of the…the fraud from the data theft or the anything. That's not the real cost. The real cost is what everybody else spends on security.

**Interviewer** 29:00  
Hmm. OK, that's interesting.

**UPR5** 29:01  
Because if you think if you have 1000 hotel chains, one gets hit, right? That's small cost, but then the other 999 are going to spend money on security. That's the cost.

**Interviewer** 29:14  
That's a really interesting angle. Yeah. Then OK, so and then question number 5 and what are the common cyberattacks that you deal with like? So I think it's more like when you are delivering this consultant job. So what are the major cyberattacks you've been dealing with?

**UPR5** 29:35  
Yeah, very much like what the list I talked about earlier actually, but a lot. OK, here's how I talk about it so. You have a…a chain of events. I think I talked. Did I mention the burglar? Did I talk about the burglar?

**Interviewer** 29:53  
No, no, no.

**UPR5** 29:53  
Then I talk about, OK, so imagine…imagine you have a burglary, OK, in the House, so the burglar is going to, first of all decide to be a burglar. OK, then they're going to choose like the region. I wanna be a burglar in London, for example. OK.  
Then I'm gonna say, well, we're, we're in London. Where should I go to do some research? They talk to some friends say ohh Hampstead. You know, it's a very nice place in London. We should focus there. OK, then they're going to do some, some, some. They're going to visit Hampstead. Maybe they're going to look at Google Maps and they're going to do some searching online. They're gonna choose some locations. OK, maybe that's an interesting street. Then I said this is an interesting house. So why is the house interesting? There's a nice car. It looks like they have good stuff inside. You're kind of hide, you know, there are some trees. That's some land behind this type of thing. They have some particular vulnerabilities, the… you know the doors are not locked properly. The windows don't have any security. There's no burglar alarm. These types of things. And then they're going to break in, then we're going to move around the house. They're gonna take the stuff and they're going to leave and sell it. So you have the series of events like this. In cyber, we call this the kill chain. Maybe you heard that phrases. So kill chain.

**Interviewer** 31:06  
kill chain.

**UPR5** 31:06  
OK, so this is the burglary…burglary kill chain.

**Interviewer** 31:06  
Yeah, I heard that.

**UPR5** 31:09  
So how do you kill the attack? You have to put layers of protection. OK, so if you're concerned about this kind of crime and you really don't want to be exposed, maybe don't live in that area. OK, it's somewhere more normal.

**Interviewer** 31:20  
Umm.

**UPR5** 31:22  
OK. Secondly, make sure that you have awareness. Make sure you have cameras. Make sure your locks are up-to-date and you know and you have a burglar alarm and so on. And lock…lock your jewellery away in a proper safe that is hidden away from thieves. OK, so you have layers of…of security. So what do we do is we take each of the common crimes. We look at the series of events, maybe there's some searching, maybe there's some social engineering.

**Interviewer** 31:48  
Mm-hmm.

**UPR5** 31:51  
We look at that series of events that's necessary. Maybe there's some malware, you know? And then we say, what are the, what are the layers that we need to prevent each of these events. OK, it failed at this one. Maybe stop it here. You fail here. Maybe you stop it there. So you have actually when you draw the picture you have like circles, right? And we call this you probably know the…the onion of security. Yeah, security onion. You know, you got the onion is the circles like that. That's where uh Tor. That's, you know, Tor the dark nets. Onion. Onion router. Yeah, the Onion Router, Tor. Yeah. So, same idea, layers of security. So that's my, that's our focus. Look, look at all the things that you have. Servers, databases, client machines, cloud. Look at these things. Think about the attacks on each one of those. Draw the onion for each one. Alright, what do we need for this one? What do we need for that one? And then you have your plan.

**Interviewer** 32:53  
Hmm. OK. Then let me see. Let's go to question number 6, but I think the question number 6 is more like.

**UPR5** 33:08  
Yeah, that's not so much for me. Yeah.

**Interviewer** 33:10  
Yeah, that it in your opinion? Like, umm, when cyber criminal breakthrough the defence and when you are for example, when I…I think now you are doing some training in e-learning to people right? And like, what do you suggest them to in terms of the mechanism for how many reduction and incident management?

**UPR5** 33:32  
Yeah. So it's very difficult to do harm reduction after the incident. You need to do harm reduction before the incident, OK? And the key things are having backups, data backups and redundant systems so that you can operate and alternative ISP's and you know various…various arrangements there, insurance, various arrangements there to make sure that you can survive after the attack.

**Interviewer** 33:49  
Umm. Umm.

**UPR5** 34:05  
And then you've got the incident management and I think the secret, the key to instrument management is rehearsal to know in advance the different scenarios and have a plan and to train people on the plan and to empower people to make decisions very quickly.

**Interviewer** 34:14  
We heard.

**UPR5** 34:24  
So it's…it's…If you're starting to call them, you know the calling um…general management at 2:00 o'clock in the morning on Sunday because of a malware infection or data breach. It's too late. OK, you should already know what you're supposed to do. You should already have authority to do it. OK, you should…you should be calling to say this happened and I've already done these things that we agreed it's done already, not can I do these things? OK? OK, because now you ask some nontechnical person to make a decision and the early hours of the morning is very difficult here. Yeah. So, planning, preparation, rehearsal and backup, yeah.

**Interviewer** 35:11  
OK. So and just you have to have the…the plan in advance and also have the backups and the redundant for the…for the servers or like whatever your…your corporations, things like that.

**UPR5** 35:24  
Yeah. I mean, so, even…even in the small. So my business, very small business. Umm, you know I have main laptop backup laptop. It's alive. Always the thinking the data then I have a network drives that I start up once a week I back up everything. Then I have for my non confidential files like presentations and things like cloud storage also.

**Interviewer** 35:41  
Umm.

**UPR5** 35:47  
And sometimes I will email something to my Hotmail like I'm working on a document. I don't want to lose it. I will just routine I will just send an email to my Hotmail with the document. So it worst case I can go to a an Internet cafe, log on to Hotmail and my document is there. And that's…that's the small, small business.  
But you know, no, you have to. You have to think like this at every level. Small to large, yeah.

**Interviewer** 36:12  
Yeah, I agree. OK, so umm question number 7 I think I'll I will have a little change of that question cause it's talk about cyber resilience. So I want you to can you tell me about like when you are delivering this training or learning to the corporation or maybe governments and police, police officers and how…in what aspect do you suggest them to increase their cyber resilience?

**UPR5** 36:28  
Umm, OK, so the types of things that we and we…we try to do these things ourselves and also encourage them. So obviously personal behaviour is very important. What are you doing on the social media. I mean, I'm very I'm active on social media because I'm, like, selling myself right. Also, I have some opinions about, you know, Ukraine and things like Gaza. I'm not hiding this, but if you're…if I'm not, you know, I'm just a studio. But if you're working in a sensitive job, you know, be very careful what you post. Be careful about the settings on your profiles. Do you even need this social media account? Because it's a way people can find you, then devices.  
You know, avoiding public Wi-Fi because of the, you know, Wi-Fi pineapple thread, that type of threat.

**Interviewer** 37:32  
Umm.

**UPR5** 37:35  
Never crossed over work and personal on a device, so it's…this is the personal device.  
This is a work device and you never mix them. Making sure that you are patched and up to date with everything. It is the very important not just the operating system.  
Not just the antivirus, but also you know every plugin in every browser, every app.  
Everything updated. Strong, obviously strong authentication, multi factor, not just the password, but if you're using a password, you know, strong password, I'll talk about you know, how…what that should look like, how you create this multi factor options, multi factor across more than one device. So it's not that you have multi factor on the same device. OK, one factor at in the next year. Multi factor on you know I log in here then I get a text message OK and then I need this pin over there. So yeah, different. So that the attacker would have to hack into two channels. OK. So, or even three, right

**Interviewer** 38:33  
Umm.

**UPR5** 38:34  
Ohh also supply chain. So you know what…Where did you buy your equipment?  
Do you know what the components in that equipment where they came from? Ummm…supply chain for your software?

**Interviewer** 38:53  
Umm.

**UPR5** 38:53  
Who, who, who? Who created the software and who did they started the contract?  
Who did they hire? Did they have the same standards of security that you have, or do they, you know, do background checking to the same level? Yeah. Yeah, I know you're smart devices because smart devices can be a threat, so you know, don't…don't have unnecessary smart devices.

**Interviewer** 39:14  
Umm.

**UPR5** 39:18  
Locations always minimize that and avoid it. If you can, some of them are very convenient, but what's the risk with the smart device. Changing passwords on new devices when you receive them. For example, I bought a I think it's somewhere over here. I bought a Wi-Fi wireless camera to... So because my laptop is over there and my big screen is here, so the camera in my laptop, I'm always like sideways when I'm teaching. So I want to put a camera on my big screen, OK? And I ordered it from Amazon and then when it came, I was like, how do I change the password on this camera? Because they come with the password, right? I don't want somebody to hack my camera, so I need to change the password. There was no instructions even on the on the website there was no…no information about how to change the password for this camera. So I just threw the camera away, right? So …I think same things like, always change their passwords and…and so on.

**Interviewer** 40:12  
Umm.

**UPR5** 40:12  
I you know, I mean, I'm just doing a little business here, so probably I'm not the best, most perfect, secure person, but this is the advice that I'm giving them. But.

**Interviewer** 40:21  
OK. But I think you…you are really careful. For me, I think I will just keep using the camera.

**UPR5** 40:27

Hahaha.

**Interviewer** 40:28  
Yeah, yeah, yeah. But that that is a actual problem. Like for example if I when I go to I I go to coffee shops to do my work a lot. So every time now. Now I'm studying like I I have more knowledge about this cybersecurity area. Every time I want to connect to Wi-Fi, I need to think about it. You know, now open Wi-Fi. So now what I do is I always connect to my phone like my phone has the personal hotspot.

**UPR5** 40:55  
Yeah. Yeah, that's that's…that's normally my advice because the 5G network is much, much more secure. It's nothing is 100%, but it's much more secure than Wi-Fi of many 1000 times more secure than Wi-Fi, yeah.

**Interviewer** 41:02  
Umm. Umm, OK yeah, but the problem is sometimes my reception is not really good in some areas.

**UPR5** 41:11  
Yeah, I know.

**Interviewer** 41:11  
So yes, so that's another problem.

**UPR5** 41:11  
Yeah, yeah, yeah.

**Interviewer** 41:15  
OK.  
Then I think numbered 8 to 10 there are more like…I want to ask you about if among your customers are there any cybersecurity firms they come to seek for your help to…to train them, things like that? Yeah.

**UPR5** 41:33  
At cybersecurity firms? No, no, I haven't. Not.

**Interviewer** 41:35  
No, no, no. OK, not yet.

**UPR5** 41:36  
Not yet, no.

**Interviewer** 41:38  
So you're you're…you're more like, more most of your customers. They are…they are like they don't have an enough awareness and knowledge about…OK, the technique?

**UPR5** 41:50  
Yeah.

**Interviewer** 41:51  
Umm, OK then among your customers, for example, some corporations and maybe some governments, like in…what do you think the… in what aspect they are insufficient the most, in addition to awareness?

**UPR5** 42:11  
Uh. Well, I don't know because I don't. I don't do any kind of audit or investigation of their…their actual security. I'm only meeting people and so it's purely so we're purely on the awareness front. So all I'm doing is…is the awareness side and actually the…the awareness is it's quite good. Ohh, what's lacking? I think in society in general is the technical education, so people are coming to their jobs without really understanding technology, OK? And I think that's a social issue and it's not just the UK. I think that's probably an issue in many places that we need…we need more accessible technical education. We need to teach technology topics in a friendlier way, and so it's not only, you know, geeky people, right, but everybody can cause there's space for everybody. In technology, there are lots of different things you could be doing that don't need, you know, coding don't need the skill. But it's too intimidating. It's too frightening. So people aren't taking those topics. So I think that's…that's actually the biggest issue for us. It's to become a more digital society, better understanding of digital technology.

**Interviewer** 43:18  
OK, then that's jump to Section G. section G is…is talking about public private partnerships in terms of cybersecurity. So you can just answer like, from your experiences. So the first question is, what do you think about the idea of public private partnership in terms of cybersecurity?

**UPR5** 43:45  
Well, I think that's already there actually, because if you look at the, you know, when we say public sector, we mean government, right? So we look at the…so you look at the public sector, the public organisations, they are most of them now…They used to have their own IT department, their own infrastructure management and everything.  
Most of them now, they outsource to the private sector. Uh…and they will have, you know, I don't know Hewlett Packard or Microsoft or somebody in there providing everything, the machines, the, the network management, the security, everything. So I think actually that is already there. Now, whether that's the best way or not, it's difficult to make a judgment. I think it's probably the best way to get IT that works. Is it the most secure IT? I…I…I don't know, but if I have to guess, I'm going to say it's more secure than before, right? But I'm only guessing I don't have any metrics. OK, yeah. Yep.

**Interviewer** 44:51  
OK, that's alright. OK. That…so when I say partnership, maybe in terms of for example, government, they will outsource the private company for strengthening their cybersecurity, but also in terms of strength the whole for example, the whole UK on the cybersecurity for example, to have the to…to have some more useful policy, things like that.

**UPR5** 45:06  
Yeah.  
OK. Yeah. OK. So that, yeah, there are quite a few things in that space, but the probably the most important one is the…this is all public information. It's the publication of the CyBOK. Have you seen CyBOK?

**Interviewer** 45:38  
CyBOK, no.

**UPR5** 45:39  
OK, so if you look for CyBOK, yeah, it's published by…it's published by National Cybersecurity Centre. It's the free document. Anybody can download. It's quite big. It's like 800 pages of cybersecurity guidance and they keep update, they just did the update like I think like yesterday they updated like every six months or something and it's…it's too big for a small business but it's very useful for you know like a cybersecurity leader in a corporate situation.

**Interviewer** 46:03  
Mm-hmm. Umm.

**UPR5** 46:15  
So this is the government gathering and it's written by like a lot of experts. OK. It's like it's not written by the government's employees. It's written by experts from across the cybersecurity industry. Uh, but gathering into one place all the ideas about cybersecurity, putting it out on the open Internet. It's available to anybody in the world who wants it, and lots of lots of lots of good information in there. So I…I usually when I teach, I usually put the CyBOK as like a…a post course reading. They're gonna take away and read later if you want to, or you can refer to it later.  
So I think that's a really good example of…of the public private partnership right there. There…there will be other ones similar but that…that for me is the biggest one.

**Interviewer** 46:58  
The biggest one. OK. And the then in terms of that kind of partnership, does that really help on the whole situation?

**UPR5** 47:06  
I…I think so. I think so, yeah, because people are actually given permission to take the CyBOK and build their training from it. I…I…I teach, I don't actually teach cybersecurity. I teach cyber crime, so I explained how the crime happens. So obviously, yeah, we talk about security, but it's not really the focus. The focus is how does the crime happen? So for me it's CyBOK isn't so useful because it doesn't talk about that, it only talks about security. OK. But if somebody's teaching cybersecurity, or maybe auditing, you know, or any of these, you know pen testing any of these things. It's a very, very useful document.

**Interviewer** 47:48  
OK, then number 2, question number 2 is like a…see as you just told me, you talk about this kind of partnership and in addition to that, do you know any other kind of partnerships?

**UPR5** 48:01  
No, I'm because I'm not...really, I'm sure there are some things happening that I don't know about, but I'm not really in that space. I don't really think about that topic, so no, I don't know.

**Interviewer** 48:08  
Mm-hmm. OK. OK. That'll be fine. And how about then when you when we talk about partnerships, right? And what do you do you think in your in your opinion in your experience because you have you have taught a lot of like maybe police officers and then corporations. So when they work together, what is the difficulty for them?  
What do you think? In your opinion, yeah, the difficulty and also the the difficulty and the advantages.

**UPR5** 48:36  
Difficulty. Sometimes it's OK, so I think I think this is true not just in the UK but probably everywhere or most places. What do you what do you often find is this is actually a…It's a problem, but it's also an opportunity.  
OK, So what you find is people will go into, for example, police or military or some other service like this and they're focused is, I'm gonna do like 6 years here and in the six years I'm gonna learn all these different things paid by the government.  
OK, so I'm gonna do all the courses. I'm gonna do all the experiences, and then I'm gonna go and join, you know, a bank or, you know, some big engineering company as the head of security or the head of something. OK. And it happens. OK. But the positive is when…when the police, when the bank has a problem, some crime takes place and they talked to the police, very often it's actually in the bank and ex police cyber person who was talking to the police. So they have a very good communication.

**Interviewer** 49:45  
Umm.

**UPR5** 49:47  
Not every time. Not always, but very often it's like someone from policing is now over here. And then when there's a problem, they speak the same language to each other. OK, they understand each other. This person knows what the case file should look like, so they will actually give the police a case file already made up in the correct format with, you know, with the correct type of evidence handling the correct way. No, not every time. OK. But I have seen that happen. So. So that's actually a positive. If you can have a flow you know from, say, policing or like law enforcement into the private sector and maybe sometimes even a flow going at other direction from private sector to law enforcement, this also happens.

**Interviewer** 50:25  
Mm-hmm.

**UPR5** 50:25  
That is a really good way to make sure that people understand same issues in the same way they communicate effectively. If you have, you know two different communities that never speak to each other and don't understand each other, then then you have a bigger problem. So it doesn't mean there are no problems. Of course there are problems, but I think it's a lot better than it would have been if they didn't have that crossover.

**Interviewer** 50:49  
Mm-hmm. OK. So then in your opinions, what do you suggest for the…the direction of for the future cooperation between the government and the the…the private sectors?

**UPR5** 51:06  
OK, my main concern is that and this isn't really a UK, it's more of a global thing because a lot of so it's an AI concern, right? A lot of the AI it's actually, it's actually from America. But I think that we need to be very careful about too much freedom to build anything. OK, to have no responsibility or accountability for what you build to even go and describe it as a problem after you built it, and then you're still building it, like Sam Altman.

**Interviewer** 51:33  
Umm. Umm.

**UPR5** 51:41  
So Sam Altman is saying, hey, I is going to destroy the world. This is a he built it, right? So stop building, OK or fix it, right? So there there's…there's it's a…it's a…it's a philosophical question, OK? And it depends on what…how you feel about this. You know, private sector and capitalism and democracy, and it's a very difficult thing to say. OK. You know, we are democratic and capitalistic, but you must stop here. OK?

**Interviewer** 52:15  
Hmm.

**UPR5** 52:15  
It's very…it's very difficult to do that in the in our system. So so there's a real danger that technologies are being developed that can cause a lot of harm and they don't have any guardrails on them and nobody seems to be accountable.

**Interviewer** 52:25  
Mm-hmm. Mm-hmm.

**UPR5** 52:32  
OK. And they can steal all the data from the whole Internet and just use it without any obligation to compensate anybody who created that data. Umm, that's my main issue right now. I think I think. We are creating some amazing things that could be very useful, but we're also creating a very dangerous space where everything, a lot of things could go wrong and I…we…we don't know what's gonna happen in the future. But I can see this could be amazing or this could be terrible. I…you know…I. Yeah, I'm not sure.

**Interviewer** 53:07  
OK. Yeah. Thank you so much, but I…I do agree with you, I think it's amazing.  
In the meantime, it's really dangerous.

**UPR5** 53:15  
Yes. Yeah.

**Interviewer** 53:16  
Yeah, yeah.  
OK, let me do some….  
OK, I think that's it.  
And thank you so much.  
And let me just press stop right now.