**Interviewer** 0:05  
OK, now we I think we are starting to record right now. OK. So thank you so much again and I'll start from Section A and Section A. It's for the basic information. So the first question I will put you in public sector. Yeah. So can you and the question number 2 is what department what you need, do you work for like your experience?

**UPU4** 0:37  
So on my experience, I've been working in cyber security, specifically within exercising, which is the simulation of cyber security incidents affecting the particular company that I work for at the minute. So the…the way that that kind of works is I will generate a simulation. I'll create a storyline essentially, and I'll work through different injects of information to try and capture lessons or recommendations. Areas of best practise, that kind of thing. And the simulations are obviously all based on reality. So they pull on different attack vectors different APTs, that kind of thing, just to try and make it realistic and engaging, and then from the other side of that I also do debriefing of live incidents that are affecting the company, again capturing that learning.

**Interviewer**1:33  
Mm hmm. OK, so then how long have you been working for in this kind of industry?

**UPU4** 1:41  
I am…so, as a private industry, this will be around 18 months and then in terms of my career, I was with the [the name of a national law-enforcement agency] before that and I did that for around four years. So about five nearly six years total.

**Interviewer**1:58  
OK. And so then what? What are your main responsibilities? Like right now or and also when you were working in [the name of a national law-enforcement agency]?

**UPU4** 2:11  
And so my responsibilities were. Currently are focused on running those exercises, so there's only myself in the in in the company and works across 100 different countries. I think there's about 120,000 people that work for us across our central company and then the operating companies that sit below that. What I'll do is, as I've said, is I'll generate cybersecurity exercises to test everything from our instant response teams and do something technical, our SOC team, our threat intelligence and so on, all the way through to the C-Suite and running exercises, everything from a regional level through to international level. Again, that's simulating the different attack vectors that we may face as a company or via one of our third party suppliers, that kind of thing. And when I was in the [the name of a national law-enforcement agency], very much the same in terms of running exercises. But the target then instead was more around supporting our regional organised crime units, going out to local businesses. All the police forces. And running exercises with them all the way through to working with the National Cyber Security Centre, delivering exercises for critical national infrastructure and again all the way from regional through to international.

**Interviewer**3:33  
Mm hmm. OK, so it sounds like you're you have a lot of experience in cybersecurity and yeah.

**UPU4** 3:41  
A lot in in relatively short time, but yes.

**Interviewer**3:44  
OK. And now let's go to Section B and Section B. The questions are all like more comprehensive. Related to cyber security. So the first question is, in your opinion, what are the major cyberattacks in the UK and also what are the modus operandi?

It can give some examples if you want.

**UPU4** 4:12  
Yeah. I mean, I think the the most common ones that we're seeing at least are the phishing campaigns and whether that would be spear phishing. And we've seen some use of AI, particularly at targets in the CEO of our company, that's not been relatively, I mean it's been relatively easy for us to spot them at the moment because AI hasn't necessarily been to the standard, but they probably would have hoped in terms of enabling their attack to to go through. But it does seem to be paired quite closely with phishing campaigns. So we'll have phishing campaigns target us, targeting us from either pretended to be one of our suppliers, or potentially it's relates to one of the events that we've got running at the time. A lot of it really focuses on the human error side of things. I think that's probably the main aim for them is to hopefully catch somebody having an off day. In terms of ransomware, we've seen quite a lot of that as well. If they have managed to access our systems, they the aim has been to then ransom the information, usually for financial gain. Sometimes if it's relating to, say, a company that has a connection to say oil or gas or something like that where that people have maybe have more of an emotional connection to it. You may see that the…the aims may sway a little bit away from the financial aspects, it might be more towards their moral compass, but that's less frequently now. I think the other thing that we see quite a bit of is crypto mining. They'll try to access one of our system, spin up some of some virtual machines and then try and mine some cryptocurrency until we've identified the risk that's posed.

**Interviewer**5:57  
Mm hmm. OK, thank you so much. When you mentioned about the ransomware, so most of the cyber criminals they when they ask when they ask for ransom, most of them do they prefer to you know you to pay in cryptocurrency or any other ways?

**UPU4** 6:04  
Mm hmm. Generally, they're looking for cryptocurrency. The obvious kind of 1 you'd expect is Bitcoin that they're requesting for.

**Interviewer**6:21  
Mm hmm.

**UPU4** 6:26  
It then it, I would say just put in my head on for my previous role. What I'd find is generally in the industry is that we didn't see whether or not companies were paying this because they didn't necessarily want to inform law enforcement because of the potential impact on share prices and so on. So we never really saw if they were paying in it, but we know that it was happening generally. It was Bitcoin that was being utilised. Now that I'm in private industry, I know from my company they would not engage with paying any ransom the demands that were made. But the likelihood is that we would see it in again. As I say, Bitcoin or something similar.

**Interviewer**7:07  
I see. OK, then let's go to question Number 2. So in the UKI, what are the major targets of the cyber attacks and also what are the reasons?

**UPU4** 7:22  
OK, so I think some of the the recent ones would be for example.  
Well, generally will be the critical national infrastructure that I'm thinking of. So within the UK that could be the Royal Mail was hit with a large data leak, some, a couple of years ago, not so much with it being a target now, but something that affected us. Not on my company specifically. But obviously the crowd strike incident that's happened recently, that's not necessarily attached to a threat actor. But again, it's something that is we should be aware of. I think with their parties being so integrated now into our system, but potentially there is risk that comes through that pathway. The…just after, remind me, sorry for the question. I went off a little bit.

**Interviewer**8:08  
So yeah, what are the major targets of cyberattacks? And and the reasons behind it?

**UPU4** 8:12  
Yeah. So I I think rarely that the major ones that as you can see are gonna be our critical national infrastructure again is what I would say. So exactly as I've said, whether it's the Royal Mail, maybe so, but more likely going to be gas, power, water, that kind of thing. Power power definitely will be something of interest. Obviously, we've seen that used previously in Ukraine with targets in power stations and so forth. I think a lot of it comes down to geopolitical strains, we'll say, obviously there's a connection to that. That's not to say, though, that you don't have somebody who has particular focussing on a target, but they they may. They may want to push forward with. I think a lot of this really is more focused on like the big game players. You know as to say the nation state backed so groups rather script kiddies.

**Interviewer**9:10  
OK, so I think this also can reflect to the third question so. In your opinion? What are the factors affecting the whole cybersecurity in the UK? And you just mentioned about this maybe some geopolitical issue or some financial gains maybe or what what else do you think or you can yeah explain more?

**UPU4** 9:37  
Yeah, no problem. So yeah, definitely. I think the geopolitics plays into it certainly. If we're seen to support Ukraine, then obviously that makes it more likely that Russia may be upset with us and therefore look to test our systems more than probably they are doing anyway as as standard. Obviously they're they're not the only nation state that's looking at that. This North Korea, for example, China and so on, obviously have similar sorts of capabilities. I think the problem that we're seeing really is probably a mixture of education and a mixture of financial support within the area and then within private industry they generally are seen to have more money to spend on this kind of thing if they want to. That doesn't necessarily mean that they do. And then with respect to the government spend inside of it, from what I saw, they obviously are trying to spend the money as best they can, but they have sets and requirements in terms of how they use the spending and contracts and so forth, but probably make it more difficult because obviously the the people that were fighting against don't have the same stipulations. And so we're always almost one step behind the attacker, as as soon as we plug one gap, they look for another way to get past us.

**Interviewer**10:53  
OK, so when you said a mixture education can use explain more about this?

**UPU4** 11:03  
Yeah. I mean, in terms of education, I don't think the if you've started the very early stages of childhood and so on. I don't think the UK necessarily focuses much on cybersecurity as they could do. I know it has been entered into the school more recently in terms of, you know, it's more focusing on safety online and it's focusing on social media, that kind of thing. But I think we've got a generational gap there where people are growing up with technology and they used to use it all the time, which will hopefully set them in a good standard. But in terms of some of our.  
That maybe my generation are older, so sort of in the 30s, 40s, 50s and so on. Then they don't necessarily as in in my experience of what I've seen, they're not necessarily as engaged with cybersecurity and potential understanding the risks that's posed. So although there are, although there is education out there from the NCSC or from, you know, like I say, free resources and so on with charities and so forth. I don't think people necessarily have the interest to look at it. I think they they browse and they use it for shopping and so on. But then as soon as something happens like a phishing e-mail, it might not necessarily understand where to report it and how to act with it.

**Interviewer**12:22  
OK, so people like most of people, they lack this kind of awareness maybe?

**UPU4** 12:32  
Yeah I will say the basic level of understanding around it is an awareness of what's a phishing e-mail looks like and so on has improved. I don't think it's necessarily that great yet. And as as things like AI make more realistic emails. It's going to become a more and more difficult.

**Interviewer**12:54  
OK. Thank you. Uh, so now let's go to section C and section C. The questions are, uh, related to cyber defence strategy. So the first question is what are the overall cybersecurity plans of the UK Government?

**UPU4** 13:17  
OK, I am…So I know that the UK Government has got a charter, the cybersecurity Charter that was set out, I think from 2022 to 2030. That is supposed to be running, which outlines the kind of aims and objectives that the UK Government has. I don't know if that's changed with respect to the government change that we've had recently, but they kind of set out some key pillars in terms of they were looking to detect cyber events, develop security skills and culture within the UK and minimise the impact of cyber security incidents, that kind of thing. I think there were five altogether, but in terms of that as a body, I know that they're pushing it through a government level and they're trying to engage with parties such as such as the company I work for through, say the NCSC exercise in the box or there's the cyber essentials work that they do for trying to ensure that companies offer a set level or have a certain level of security. As a baseline, but in terms of whether or not that's enough is yet to be seen, it's it's only been running for a couple of years. As I say, it's supposed to run until 2030, assuming it hasn't changed.

**Interviewer**14:33  
OK. And then how do you think of these plans? How do you evaluate them?

**UPU4** 14:40  
I think the governments. From what I've read of it, I think they it makes sense the plan that they've laid out, I think the difficulty that they have is engage in private companies in investing money within cybersecurity. At the end of the day, companies are there to make profits and securing their data and so on. They have to do it from a legal standard to a certain point, which I think a lot of companies try to do, if if they don't already do that. But in terms of the added level of security, such as cybersecurity exercises similar to what I do, I don't think companies generally do that, which would have actually, for example, the crowd strike incident recently, if they had, if a company had been affected by that and they've drawn simulations, tabletop exercises, that kind of thing to look at a response, the impact that they felt may not have been as impactful, I suppose. And unfortunately, I don't think companies are necessarily engaging with that as as much as they should do. I think the NCSC’s exercise in a box, for example, that is aimed at small to medium sized companies, so large, large…you know, companies such as where I'm based, where it's international and so on. And I've got a large number of staff. I think it kind of left to your own devices that you should be paying for that though, which I understand wouldn't make a lot of money, but. I don't know necessarily for the health to accountability if there is a large data breach, if it's…Yeah, if it there may be more that could be done.

**Interviewer**16:18  
Mm hmm. OK. Then let's go to question number 2. Uh. So what are the current cyber threat precaution strategy and of the UK government?

**UPU4** 16:23  
Mm hmm.  
So I think that that falls back into the government's cybersecurity strategy that I was mentioning that came out 2022 to 2030. I think that's the main strategy that we've got in play at the moment. I don't. Do you want me to expand on what kind of covered already or?

**Interviewer**16:56  
Yeah, like. So what I was what I want to ask is. Yeah, about the. Because the the precaution and the prevention and also, yeah.

**UPU4** 17:12  
So I know for example in the NCSC for example, they had a a prevent team that would literally the whole role was about going out and educating people.  
They and trying to get to the people who maybe are heading down a route of criminality and stopping them before they do something that is gonna potentially affect them in the future and. They used to be, from my understanding, a case of people believe that if you prove how good you are as a hacker and you could do XY and Z that that might lead to a job in industry, that kind of thing. That's not really the case anymore, because why would you give someone the keys to the Kingdom as it were, if they've shown that they've morally questionable?

**Interviewer**17:49  
Mmm.

**UPU4** 17:58  
So the prevent team will go out and as I say, try to speak to these people before that and then try and put them down the correct lines of education and then bring them into industry, assuming no criminal offences are taking place. So I think that was really good. They they had some training that they would send out again around certain times like the summer. Now they'll they'll do a an online course for children to take part in and try and put up and down that path as well. I think then in terms of the net, the takedowns of like websites and so on, you would find that if you search for certain things, I'd like say, if you were looking for…some DDoS, for example, support. If you were trying to make your own, or maybe you were trying to buy it from a vendor. What the [the name of a national law-enforcement agency] would do is have the websites would be flagged up that you know this is now under control of the at the [the name of a national law-enforcement agency]. What you're looking for is breaking the following pieces of legislation, give them information. I know that they were branched out in Reddit as well and they were monitoring some of the hacker conversations that took place on there and openly saying, you know, we are here and we're aware of everything that you're doing that had mixed responses. Sometimes people didn't believe that they were actually the, you know, the police to the agency and then otherwise that time it did see the numbers of people in those conversations falling away because obviously they were…they were concerns about the police being involved then. So I think we…we are trying to take things. It's very different cybersecurity because if you think from a legislation point of view, if it's drugs or violent offences, that kind of thing, it's all very much legislation that stood for hundreds of years, potentially or a long, long period of time. But for cyber, it's moved so quickly that the legislation hasn't necessarily caught up with it. So the concerns that we've got are that the legislation doesn't meet necessarily what we need now. I'm talking about potentially you have very short sentences if found guilty. So to try instead of relying on the legislation, which is maybe quite weak, instead of focusing on trying to get into people early. To do that, we'll have to do something that is a little bit different for the police. And I think, which is, as I say, go into Reddit and so on, where traditional policing would never end up in there. I hope that makes sense.

**Interviewer**19:59  
Mm hmm. Yeah. And that makes sense. So I think you also mention, you know the third question because I was, I want to ask you about. In your opinion, what can be improved? You know? Yeah, of the problem you just you just mentioned so.

**UPU4** 20:36  
Mm hmm.  
I think really. Yeah, it a lot of it is down to funding a huge amount comes down to that because whether it's a case of us trying to stop incidents taking place. I bringing in new tool sets so you know education or whatever it is that we're trying to do. Unfortunately, everything costs money. So the financial side of it has to be taken into account. So I think more money and investment needs to be to be put into that. I think engagement wise with schools is good. I think it will be useful for people to almost have an education piece targeting adults that's free, maybe from the government perspective that might be in place already that I'm not aware of. I don't know. But, something like, you know, if you're talking the children, that's great. But in terms of we've got several generations that are still navigating around the Internet and so on that aren't necessarily paired with basic cybersecurity. And then. I think, really the aim for the UK is that we want to be seen at a Nokia. Kiev Starmer was saying at the other day that we want to be seen to be the big player again and really focus on cyber is the future. I think that's that's very important for us moving forward. We're very reliant on IT as as we've saw with crowd strike recently. So it makes sense for us to invest into jobs in the UK and keeping that knowledge within the UK. I'm obviously working with other countries to do so and developing in a friendly manner, but ultimately we don't want to lose those skills if we are losing people to other countries because they see those jobs to be more favourable.

**Interviewer**22:31  
So, create more job opportunities and puts more education and targeting at adult to raise the awareness.

**UPU4** 22:41  
Yeah, I mean I I I see quite a lot. I mean for example, if you're working in cyber, you're probably aware of it, you bring it back and talk to your family about it and so on. But unfortunately, especially if you go into the kind of more strategic roles, again, I'm not speaking specifically about any company, what they the strategic role is very much focused on leading a company in a certain direction and so on. And obviously the amount of data that they have access to and how busy they are, they make great targets, obviously, whaling opportunities and so on. I think they're the ones that I would definitely be looking more at within the companies, I would also be looking at anything that's considered a crown jewel system or a crown jewel team. I, HR got an absolute wealth of information there, you know, make sure that they're very much aware of the requirements around cybersecurity.

**Interviewer**23:38  
OK. Then let's move on to Umm question 4. So before we were talking about the precaution and prevention and then how about when we are facing the ongoing cyberattacks, what are the strategies of the incident response?

**UPU4** 23:58  
OK. I so incident response wise really at least from what I've seen you wanna get as much information that's relevant as quickly as possible. So linking in with any, if you're lucky enough to have a threat intelligence team or threat hunting team looking for those indicators of compromise, trying to identify them as quickly as possible. Potentially then it it very much depends on what the incident is. But then look at your mitigation opportunities, providing guidance across to whoever the affected party is, making sure that you gather your digital forensics. So for example, it's something that we quite often see, not necessarily again, but in our company, but with when I was in the agencies, we would turn up to a site that someone was been affected and we provided those sort of guidance that were possible. But the problem was then you…something had happened where there may be a laptop had been wiped and reset again, so you'd lose that digital data that would be useful for a forensic perspective. In terms of the initial response absolutely you want to carry out all those sort of steps and make sure things are back up and running as soon as you can. But making sure that not gonna be affected again in the future by the same kind of incident. I think the way I see it is that as much as you can do all the physical and the…So say, for example, you've gone through and you've done all the IoCs (Indicators of Compromise) you've brought in the relevant teams to get the job back up and running again. It's the education piece that needs to come after that made. Essentially, if you if you don't educate, then they're likely to have the same issue again, even if you have fixed it, whatever the issue might be for that particular instance.

**Interviewer**25:44  
OK. And then? How do you see how? How do you think about these strategies and what can be improved? Or to make it better.

**UPU4** 25:58  
To make it better, I think the with incidents that the first thing that you need is to identify as soon as possible. The earlier you identify it, the easier it's gonna be for you to hopefully be able to mitigate any future risks, but also to stop the incidents in its track. So whether that be again educating people to understand what it is that they're looking for that they shouldn't be clicking on hyperlinks that have been sent by somebody that don't know and haven't…at least done some sort of, you know, due diligence around. When they identify something that isn't normal. And that they could report it. Again, they don't necessarily report it, but obviously quite a lot of people, they've just delete an e-mail or…or something like that. And then I think.

**Interviewer**26:34  
Mm.

**UPU4** 26:44  
The big one, no matter what it is that you work, is communication. It's just it a lot of the time when we're working on the incident, it could be that there's we want to focus on executing something in particular, but unfortunately we have different perspectives on how the incident should be run. It might be that an operating company, for example, has a CEO and a deadline that has to be delivered.  
Unfortunately, an incident response team's focus is making sure that that risk is mitigated and they don't necessarily meet at the same point, so therefore communication's absolutely key. And unfortunately I think just in general, cybersecurity and otherwise education…uh…sorry communication and it could be improved.

**Interviewer**27:30  
Mm hmm. So, the communication?

**UPU4** 27:34  
Yeah, whether that's whether that's pathways or whether it's delineation of responsibility between teams, you know, if the essentially just having your communication plan laid out whether that's the external partners, internal partners, it really makes a huge difference.

**Interviewer**27:49  
OK. And then let's move on. And So what about the post cyber attacks? What are the reflection measures?

**UPU4** 28:03  
So before I work I I'll offer a…post incident debriefs. So what we'll do is complete a full debrief with all the the relevant partners that we're within that incident. So that could be where initially began all the way through the incident response threat intelligence SOCs and so on, all the way through to potentially seniors that have been involved in it again just depends on how the incidents is developed, what we'll do then is have a discussion based review of what happens, who took what steps, why they had those steps in mind, what potential risks they saw, that kind of thing.  
I'll document it all down and then from that I'll provide some recommendations as to what steps should be taken moving forward and as well as that I'll highlight any good work that's happened, because it's important to reflect on on it from a positive as well, because it's not always going to be negative. And what we'll do then is capture those recommendations and we'll put them out to relevance. I suppose relevant owners or risk owners, and they will be charged with delivering whatever those recommendations are. Because the way that I work is it's a recommendation, they don't necessarily have to deliver it. It might be that there's some sort of blocker in the way. Again, it could be financial, it could be that we don't have a tool that does that yet. It could be that that procurement is required, but with them have regular updates and ensure that they are at least written down as a risk that we are happy to carry on with on the on the understanding that we're trying to fix it.

**Interviewer**29:19  
Mm hmm.

**UPU4** 29:38  
Otherwise, we'll close off the risk once we've achieved whatever the recommendation was and that then feeds back into exercising and we'll run a cyber exercise to see where our improvement is and then we'll continue from there. I think obviously there are other elements that you have in the companies outside of that, whether that be risk registers that we keep patrol of the risk more centrally. And again, we have a culture team in our company. So that will, you'll see some training that will come out around that. So we have regular phishing simulations and so on that will run through. But if there is a large scale event for example, I'm gonna have a load of corporates and colleagues arriving, then we'll also have something focused around that, whether it be, you know, personal security, thinking about Wi-Fi usage and that kind of thing and yeah, so it's it's very much targeted and depends on what time of year it is and what's happening.

**Interviewer**30:32   
Mm hmm. So it's all connected. Uh, from the prevention and then the incident response and the and the post cyber attacks and then to have some reflection and then to to again improve your prevention and then precaution strategies?

**UPU4** 30:52  
That's correct, yes.

**Interviewer**30:53  
OK, then let's move on to question eight. I think you had mentioned before, so how do you describe the awareness of the cybersecurity among the general public?

**UPU4** 31:10  
Yeah, I think it's improving. I don't think it's necessarily good at the moment. I think it it's it will become better as the new generations we used to brought up with technology at the hands all the time, they will be more aware than my generation was and I'm probably more aware than like previous generation was. I think the problem you've also got is as I've mentioned is AI may play a massive part in this in terms of how believable things are. We're already seeing as I mentioned.  
AI being used for phishing developments to make something more realistic, AI videos and so on. Deep fake and so on. It's it's I think it's a case of education is improving it but it's whether or not our education is keeping up with the technology.

**Interviewer**31:59  
OK, so we need to keep the…make the education keep with the with the technology involving.

**UPU4** 32:07  
Yeah. Yeah, I think so. Make sure the general public are more aware and keep offering these opportunities for people who are interested to be educated.  
And bring and as I say, as we bring more people hopefully into the cybersecurity.  
Workforce that will naturally help as well, I think so. As we talked about before, employment within such a field will definitely benefit it. I think probably something that should make mandatory probably for all companies is that there's basic cyber security training on the job and have that regularly at least yearly. If not, you know, on boarding, off boarding, you know key points through the calendar, that kind of thing. The problem that you have there is probably engagements because not everybody's interested in cyber, never mind cybersecurity.

**Interviewer**33:00  
OK. So let's move on. The question now is, what are the current governmental plans of the cybersecurity education for the general public and how do we evaluate these plans?

**UPU4** 33:14  
So I know I'm, as I say, from from what I've seen is it's been brought into schools. I know that's some of the children that I'm aware of are going through basic cyber in terms of like media focused though it's protection online, that kind of thing moving into this kind of industry side of it. The the one I probably use most of the time, which is particularly of interest to me, is exercise in the box, which has been by the NCSC, which provides really easy to access cyber simulation. It's very much generic, it's off, it's off the shelf in terms of the scenario it provides. But the idea is that you run it, you have your discussion, it gives you outline of all the questions that you might want to ask in there and it drives discussion. It's very much the idea of you have this box that you open and it's got everything you need to run a basic cybersecurity simulation and get that discussion going. I think that's a really good tool. It's completely free. And that's something that I certainly would recommend people have a look at because ultimately it gives you a sandbox situation that you can work through that. If you make a load of mistakes and people don't know where the policy is or they haven't got the the knowledge that maybe they should have, it doesn't matter. You've identified a load of learning points from there that you can then work on and it's not done in a live incidents.

**Interviewer**34:43  
OK, so it's on NCSC website?

**UPU4** 34:46  
Yes, that's right, yeah.

**Interviewer**34:47  
OK, OK. So it's more for like individual or also they offer some this kind of simulation for a company or organisations?

**UPU4** 34:58  
It’s more for small to medium businesses.

**Interviewer**35:01  
OK. then let's go to question number 10. So, in terms of the, you know, attract the future cybersecurity talents, what are the governmental plans, you know, the cultivation, the education or some plans either to to educate them, cultivate them or to attract some talents.

**UPU4** 35:36  
Good question. I think from again, I'm. I'm gonna go back to the kind of work that we've done in. So, in the company at that I've done, it's not actually government led unfortunately. It's more that we're going into schools and offering opportunities for them to come see the advertising world. And as part of that there is a cyber that we'll talk about whether it's design and so forth. So it would be good if the government is offering support for that. I'm not aware if they are in that in that if that's literally because the company would like to support the local schools that are around us and potentially that leads to cultivating jobs and so on. I know when I was in my old role. And in the [the name of a national law-enforcement agency], obviously that is government based. And as I mentioned before about the prevent team, they were going out and speaking to people who are committing offences and hopefully stopping them before committing a crime that is going to impact their future. And then they will guide them down a route into a proper education and then try and get them to use their skills for something in the future, like a like a job which is, say, or maybe a hobby or so forth. And they had the side of the skills events. I think they're over in the summer where kids could go on and compete against each other. And it's kind of gamified cyber scenarios, whether that be they have them writing some codes to make it something happen or whether it be more than responding to an incident, that kind of thing. They did that up to a couple of years ago. I don't know if they're still doing it anymore, that that may have stopped.

**Interviewer**37:06  
OK. And then what do you, in your opinion, what do you suggest for the future?  
Governmental plans on this.

**UPU4** 37:18  
I think I would like to say something similar to. So where they have basically people are, you know, put into a load of different sports. They try and figure out what you're good at and ultimately that's the kind of sport that they'll put you in. And they build these great teams, whether it be rugby or swimming or so on. And it's because you're naturally more maybe gifted towards that. I don't know exactly how that works in terms of, you know, choices that the children actually want to do, whether they want to do it or not. But if you had something similar where you'd be an assess normally on your English, your maths and science and so on before you move into school, you know, if there's somebody with a natural interest in it, is that being necessarily looked at?

**Interviewer**38:04  
Mm hmm.

**UPU4** 38:04  
I know that you'll look at things like, for example, people, at least when I was going to school, you would direct people with a particularly good…particularly good at maths or going to a higher set. You might be in the top set and obviously a bit more challenged. It might be that if you're particularly good with languages you'll go into learn French or German or Latin, so why can't IT be part of that as well?

**Interviewer**38:29  
OK. Yeah, good angle. Yeah. OK, so let's go to Section D and Section D it's about a public-private partnerships on cybersecurity. So here, when I say private sectors, itt means the kind of like cybersecurity provider.

**UPU4** 38:50  
OK.

**Interviewer**38:50  
Yep. So the first question is what do you think about the idea of public private partnerships in terms of cybersecurity? And does that really help to improve the cybersecurity?

**UPU4** 39:07  
Yeah, I think I think it has positives and negatives, I would say. In terms of positives, it's it's useful because you have a company that can provide you a particular service that they are targeting either maybe it's intelligence or maybe it's like I say your particular focus is on.

**Interviewer**39:12  
Umm.

**UPU4** 39:28  
It's like crowd strike you've done. You know, they they've really cornered the market. They've sharpened their skills in that particular way, and they're all gonna be better at doing that job potentially than I am in my role as a small team with far less funding and so on. So it can be great to provide us with tool sets. The concern that I would say I have is obviously with CrowdStrike recently is if it goes wrong, you impact a huge amount of people and it's what comes on after that. You know, I think with the CrowdStrike side of things, people have potentially died because it's affected hospitals. You know, people couldn't fly. There's all those sort of knock on effects, so it's not perfect. You have to really rely on them, but they have got the security is absolutely you know as as best as it possibly can be. And even then with the best will, you know you can make a mistake, you can have an error. I think this was literally just a an update that got pushed out and it wasn't quite ready that kind of thing. The other side of the coin as well is that ultimately if you're bringing in a third party company, they are doing it for financial gain. That, that's. That's what they're interested in. And if you want to make as much money as you can as a business, that's generally what your aim is. Then you will look for ways to find where you can make savings. And that doesn't mean that the product that you have at the beginning is necessarily what you get, you know, in a few years time. And it's. Yeah, it can be complicated.

**Interviewer**40:57  
OK. And then do you know any of the current this kind of cooperation, mechanisms?

**UPU4** 41:06  
For the company I work for, you mean?

**Interviewer**41:10  
Yeah. Or the just in general, have you heard about anything? Yes, you can tell me about maybe your company, like in general.

**UPU4** 41:23  
In general, I mean obviously there's a lot of use in terms of Windows products for example. Where everybody uses them and whether you maybe you'll find some companies will use an Apple derivative as well. But generally you know we're all rely on Word, Excel and so forth. But we have some sort of antivirus that we need to put in place whether like you know there's all loads of different brands that potentially can use for it. So there is…In general, there is a lot of support in that sense to allow us to complete our jobs and you know our our personal ambitions. I think though what we're probably going to see more and more of it is that introduction of AI that's going to be leading into new opportunities, but also again it opens the door potentially to new risks.

**Interviewer**42:18  
And then when you were working in [the name of a national law-enforcement agency], did you…have you ever cooperated with the cybersecurity firms that kind of cooperation?

**UPU4** 42:23  
So not with the agency. All our stuff was bespoke and I can't really go into those details just because it's sensitive data.

**Interviewer**42:40  
OK, I understand.

**UPU4** 42:42  
I am, but in terms of what we were using, yeah, obviously we had some of the core stuff you'd expect we had to write documents somewhere and so on and blah blah blah. But we didn't necessarily engage in the creation of anything that I saw. We did use…which the contractor I believe has ended now. We did go through a massive labs for simulation and training, that kind of thing. We did work with them on creating some simulations that were going to be useful for us. So although we kept all the data and so on, we use their platform to create something that was a bit more involved I suppose, in in the scenarios people could get a bit more hands on into into the simulation. So there is elements there where that's crossed over. And actually I think the CEO of Immersive Labs is format. I'm going to say former GCHQ. So you do see that elements where someone starts in the government similar to myself and then shifts to private sector, if that's kind of what you're thinking.

**Interviewer**43:21  
Mm hmm. OK. And how about now? I know you're working at private company right now, do you work with the governmental institutions?

**UPU4** 43:55  
And so we, we will work with the government in terms of anything that we're legally required to do. We do… cause I'm working at advertising sector. If the government in full support with advertising, I'm sure that the company would listen to potential opportunities there or you know go through the the usual protocols that you would have to for it. But in terms of working directly with them, not that I'm aware of now.  
I think again with the private companies, what you'll find generally is if you get…if you are thinking about safe, please send GCHQ again. They don't generally engage with them because there's a risk as far as the company's concerned, is that if they're affected by an incident, it'll affect their share prices and then reputational damage and so on.

**Interviewer**44:45  
OK. And then let's move on. And so in terms of this kind of cooperation, what do you think that the governmental institution can contribute to it? And also what …what can the private sectors can contribute to these partnerships?

**UPU4** 45:07  
What I think I know that sound the governments and for example CrowdStrike and so on. I've shared information from an intelligence perspective that they they all work together there 'cause they have their own separate intelligence streams, but actually CrowdStrikes is very good. But in terms of what level they're working, obviously I won't go into too much details there, but they're not going to be the only ones that share intelligence. I think that's the big thing is that actually from from an intelligence perspective specifically, the more that you can have from the difference partners as well as governments, then the bigger your intelligence picture is. Therefore, if you can evaluate and handle all that data, you should have a better understanding of that threat landscape. That's…that's a really good opportunity for the government and for private industry. I think specifically I think if you go into more building out platforms or tool sets and so on for the governments via a third party, then you kind of as I said before, you can get some really, really good tools.  
But you can also get somewhere the more focused on making the financial gains rather than the quality of the product.

**Interviewer**46:15  
Mm hmm. OK. And what do you think the, you know when they are working together, what are the the difficulties they normally face?

**UPU4** 46:30  
I I think there's probably one will be getting the information that they require. As I say, if there's obviously difference and categorisations of data within the government, so they can't necessarily share that with them because it's sensitive and then it's how you break that information out. Some information you can break out from a high level down to a lower level and then share with the third party. But that's going to be quite limited and you may not get all the context around it. Alternatively, you can then bring the third party company in and go through the relevant clearance and so on, and then you could share the information, but that is quite a slow process and it's expensive and you know it's…it's trying to find a thinking balance in between the two.

**Interviewer**47:16  
Mm hmm. Hmm. OK. And then in the future, what do you and what direction do you think they can work together in terms of the partnerships?

**UPU4** 47:30  
I think the biggest one is looking at how the good work together towards. Again, intelligence that's always going to be changing and developing as with those new techniques coming out. So definitely looking at intelligence specifically, but also the use of AI and how that could be utilised by governments, whether that be, you know, it's looking at photographs and trying to find a person who's missing, for example, or it could be that it relates directly to something more cyber focus than it's like a. You know, here is an example of a code that we need to…ummm look for a particular floor in that you know and then utilise that like we've seen with previous incidents that you look for a particular key. Maybe I I can assist us with that. It's…I think when you bring in third party they they essentially have new ideas outside of what necessarily the governments have because they don't. The government doesn't have the funding and therefore necessarily the reach that those third party companies have. And I think that's where you'll you'll see a lot of growth.

**Interviewer**48:38  
OK, so bring the third party, engage with a third party to have the how do you say the more broad…umm angle and view of this cybersecurity. And then also...

**UPU4** 48:54  
Yes.

**Interviewer**49:14  
OK. And I would like to ask more about the information sharing. Do you think the information sharing between the public sectors, I know the governmental institution and the private sectors they are equal or like they are they sufficient umm about the cyber security, yeah?

**UPU4** 49:18  
I would say probably…About cyber security. I think it depends what angle you're looking at. If you're talking about generally just kind of recommendations and this is kind of the threats that we're seeing. Potentially though, yes, they are kind of equal. If you're talking about in terms of reporting issues or incidents, that kind of thing into government and saying we've been hit by a particular incident, then no, the companies do not tell the government's necessarily the whole picture of the what's happening because as I said, it would affect their…value of the company. I think unless it's a large scale incident and they feel like they necessarily have to, that's when you'll see a lot of companies will start to be more engaged with it.  
I think as well with the governments, they can't necessarily always share the information because obviously as we've said before, it's it can be sensitive.  
And we need to protect sources and so forth.

**Interviewer**50:20  
Mm hmm. Hmm. OK. OK. I think that's it. Thank you so much. Yes. OK. So, and let me turn off the recording.

**UPU4** 50:27  
OK. You're welcome.