**Interviewer** 0:05  
OK, now we are. We are recording right now. OK, so let's get started so. So for let's go to Section A, Section A. It's only the basic information.  
So for the first question, I will put you in public sector because you have the experience of working in [the name of a regional police force] for many years. OK. And so the second question is. What unit do you work for when you are working the [the name of a regional police force].

**UPU2** 0:48  
What unit did you say?

**Interviewer** 0:50  
Yeah, unit and the department.

**UPU2** 0:52  
Oh, unit. Oh, sorry. Oh, OK.  
Well, lots of different ones. So how do you want me to answer that? Do you want me to give you, like, a a an idea of what my resume looks like or?

**Interviewer** 1:06  
No, that that's all. I just you can just kinda mention what what you were doing you you were responsibility.

**UPU2** 1:14  
So so I was a senior detective responsible for approximately 100 officers. So dealing with major and complex and serious investigations, ranging from homicide, child abuse, cybercrime, counter terrorism and serious organised crime.

**Interviewer** 1:53  
So then. And how long have you been working for, you know, for the police force?

**UPU2** 2:03  
So I I worked for the [the name of the national-level police force] for a year and then I worked for [the name of a regional police force] for 16 years. So in in total I work for the police for 17 years and actually I don't know if you've realised, but I…I don't work for them now. I work in industry now. I'm work, I work, I work for a private company. But yeah.

**Interviewer** 2:09  
OK, yeah, I…I actually went to your LinkedIn profile. So yeah, you just you just changed to the industry recently.

**UPU2** 2:32  
Oh. That's right. Yeah, in in February.

**Interviewer** 2:39  
OK. So specifically on cyber security, like the consultant?

**UPU2** 2:45  
Specifically, yeah, yeah.

**Interviewer** 2:46  
OK. So then I think the the following question will be you know you can just answer according to your experience, both from the the police workforce or the the current current job.

**UPU2** 3:04  
Yeah, sure.

**Interviewer** 3:05  
OK, so let's go to section B, section B. So we are just going to go through section BCD. That's it because yeah, the public sector. So and the first first question is? What are the major cyberattacks in the UK, in your opinion, and what are the modus operandi and you can also give some examples?

**UPU2** 3:33  
So the United Kingdom is essentially at war with a number of nation states on the in the cyber round. So, probably since at least 2015, I would say, there has been significant well-resourced attempts to cause problems and disruptions to all aspects of the UK government, economy, you name it. And so, on a daily basis, government, both government and industry, are facing attacks in the form of, you know, all the traditional things. So, ransomware, you know, phishing, DDoS attacks. You know exploitation of the various sort of zero-day issues that that emerge, but it's relentless and the reason for that is…is because certain other nations have the…have had the foresight, the money and the resources to invest in capability that either allows them to undertake these activities en masse, or devolve in…in…in the case of some other organisation or some nations devolve that responsibility to organisations. So, for example, you know the…the Russian state doesn't necessarily employ all of the people that are directed at carrying out cyber attacks on the UK, but what they definitely do is turn a blind eye or fund those organisations who effectively operate autonomously. That stands in contrast to other nations who are just have much more strategic foresight and have invested in, you know, huge manpower, you know.  
Of people that are able to do that sort of thing. So yeah. So what…what is this…what is the overall strategy? Well, it's just constant. It's just to constantly keep the pressure up to frustrate the UK Government, the UK economy and all the rest of it. So. So that's the top end stuff. But in addition to that, you have the Internet has allowed the exponential rise of criminality and exploitation in many other different ways. So. So if if you put it this way, if you switched off the Internet, if you had the ability to switch off the worldwide Internet, OK, today. You would. You would do away with most of the crime that occurs in the United Kingdom because if it's not, either completely pause through the Internet. It's enabled in some way, so even if you think of like nowadays, right? If somebody, I don't know, if somebody wants to steal something, they might be using the Internet to…to look at how they're gonna steal it by looking at the building security. Or they might be using the Internet to sell the goods once they've stolen it. Or they might be using the Internet to target the victim because the victim's an old lady or whatever. So you know, in the case of, like, romance frauds and things like that. So. So the point is, is that the the technology has made crime increase exponentially in a way in which the UK just doesn't have the money or the resources to effectively combat. So it's got all of that going on.

**Interviewer** 8:52  
OK, thank you. So do you think that Internet is kind of like is the tool for the criminals to commit crime or do you think it's because of Internet they have kind of like an the new new crime to commit?

**UPU2** 8:52  
So so it's both. So there's no. So the Internet no doubt, is one of the greatest things of our civilization. You know of our global civilization, but at the same time it is the means by which so much harm is caused. So. You know, I'll give you an I'll give you an example. This is my belief this isn't based on any facts and figures. This is just anecdotal experience, right. You take the issue of child sexual abuse. Umm. Before it became readily, Well, before it became possible for people to go onto the Internet and access indecent imagery of children, the numbers of…of people that may have committed that kind of crime was much lower. But because it's available to you and it's easy to access and most of them think they can access it without getting caught, what's happened is, that is, a phenomenon has grown exponentially. Right. And it's to do with that the, the…the you know, the Internet and technology gives people that ability and it's the same with if you talk about high end stuff, hacking, you know, that it as technology advances it, it all it does is creates more opportunities for people, for whatever purpose, to take advantage of vulnerabilities and exploit those vulnerabilities.

**Interviewer** 11:00  
Mm hmm. OK. Yeah. No, I agree with that actually, so. And and then let's go to question number 2. So I think that's kind of reflected reflects what you just mentioned, so. In your opinion, what are the major targets of cyberattacks or like, are there any specific industry they are more easily to get targeted.

**UPU2** 11:31  
So so there's a difference between those that would be on the wish list and those that are more easily targeted, right? So if you put yourself in the mind of a competitor, a nation state actor, then, the…the top ones that you want to target are gonna be defence. You know, defence industry, defence companies, the Ministry of Defence, Military.

**Interviewer** 11:58  
Mm hmm.

**UPU2** 12:04  
If you can breach and you know another country's military networks and sit inside there undetected, gathering intelligence and information, then that's that's great, right? But more than that, you've got anything that gives financial advantage. So, you know all of the kind of investment management organisations and the banks and all these people, you know that they are…they are significant prizes if they can be breached. But anything that has major financial could cause major financial impact in a competitive advantage where…I'm not talking about, you know, disrupting because, you know, thankfully, the people that are in these different countries are smart enough to realise that if you if you killed the UK economy somehow, that would have a knock on effect around the world. It wouldn't just cause problems for the UK, it would cause problems for everybody. So there's a little bit of intelligence that goes into what they what they do. But…but it's about stealing and acquiring things you can then use for your…for yourself. So those that's probably the two biggest ones and then government. So obviously anything you can do to get inside government and understand what's going on. But in terms of what are the most common places you see it, I think in the UK it…it's mainly public sector and medium to small businesses.  
Oh, I've lost you. So I've you back.

**Interviewer** 13:55  
Yeah. Sorry, I just I changed the…the Internet. Yeah.

**UPU2** 13:56  
All right. OK. So in terms of what I was just saying was in terms of in my opinion in terms of where where gets attacked the most often, it's more public, lower level public sector, hospitals, schools, you know, small government departments, things like that. And…and small to medium businesses. And the reason for that is simply because they don't have the money and the resources to make sure that their security is top notch.  
 **Interviewer** 14:34  
Mm hmm. OK, so it's also depends on their level of security, their awareness and also their. Yeah, their defence. OK.

**UPU2** 14:40  
Yeah. Definitely. So. So I'll give you an example very quickly.  
We have a real problem in this country of schools being subject to cyberattacks. And and if you know how the system works in the UK, you think, well, why on Earth would that happen? Because schools don't have money, so they're not good targets for ransomware. And yet constantly they are subject to ransomware attacks, but you're never going to make much money from trying to ransom schools. They haven't got it. And yet it happens a lot. So it makes you wonder well, why? Why do people do it? But the answer is, and this isn't this, this isn't state sponsored packing. This is this is criminal groups just doing this. And the reason they're doing it is because it's easy for them to do. No, no reason more than that.

**Interviewer** 15:48  
Mm hmm. Mm hmm. OK, how about the charity 'cause? I also heard about the charity. They are also the targets for cyber attacks.

**UPU2** 15:58  
Beyond my personal knowledge, but I wouldn't be surprised because again, the problem with charities are although they…they have…some of them have high turnovers in terms of revenue. The reality is, is they don't have a lot of cash. You know that. What they what they get in versus what they have to then payout is very close. There's no profit to be made or. So so yeah, I get. So again, I would imagine that if you walked into most charities, there's cyber security posture or.  
Their general awareness of cybersecurity is quite low.

**Interviewer** 16:43  
Let's go to question number 3. So in your opinion, what are the factors affecting the cybersecurity in the UK? It could be political or like, like you said, awareness anything you think it's affecting the cybersecurity.

**UPU2** 16:56  
Uh. So the…the first, the first one is, no matter how good you get at cybersecurity, someone that is determined to get into your system will eventually get in because the way technology evolves and moves, it's so fast that you can literally blink and all of a sudden in a split second there's a new vulnerability. Somebody will find that vulnerability and they'll exploit that vulnerability. And then before you know it, you're in the next Ticketmaster or the next Disney or the next, whoever, right? Suffering the consequences.

**Interviewer** 17:47  
Mm.

**UPU2** 17:48  
So that's the first thing. So no matter what you do in the UK, you're always, always, always going to be to a certain extent behind the curve. The second but…but…but to answer your question, I think the problem…one of the biggest problems in the UK is….a lack of…We're starting to get more switched on. We're starting to understand more, but what it has been is an issue of a lack of education and understanding on how important these things are. I'm gonna say something. So do you. Am I right thinking you are you from Taiwan?

**Interviewer** 18:27  
Yes, I'm from Taiwan.

**UPU2** 18:28  
Right. Please don't be offended by what I'm gonna say, but I'm gonna. But what I'm saying is I really admire the Chinese…in that. They have. They don't think about a problem that's in front of their face and react to that problem. What they do is they think 30 years in advance. So at some point the Chinese Communist Party. People within that organisation looked at the way technology was moving and said, you know, we need to make sure that that we put mathematics and computer science and programming and coding and all these things at the heart of what we deliver in our curriculum because in 15 years’ time we will start to see generations of highly skilled, highly educated, competent individuals that then the party can use for the benefit of China, right, good, bad or indifferent, right. It's all about perspective. The UK doesn't do that. The UK goes, oh, there's a fire. We need to put it out. They don't go. Oh, we might get a fire if we don't deal with this situation and think in advance. So that's a big issue for the UK and is one of the causes is one of the main reasons as to why we are, you know, because people just have, there's a lack of consistent understanding, education, interest in cybersecurity. And so we are. We are very, very much compared to other global powers. We are very, very behind and we can probably never catch up.

**Interviewer** 20:12  
Mm hmm. OK, so are you saying compared to like China or like Russia, the other countries or?

**UPU2** 20:29  
So so I think, yeah, I mean compared to so Russia I think is different. So Russia I think they they haven't necessarily invested to the same degree as what the Chinese have. But like in North Korea for example, you know my understanding is is that you know they've gone along the same lines. So. You know, we…we, you know and even in India you know you go to India now you know there's so many people getting into cybersecurity and information security and having those skills and…and a small island with a population of, you know, 70 million cannot compete in any way, shape or form with that level of strategic planning organisation, you know. So we are constantly, you know going to be on the back foot unless something very dramatic changes where we basically, you know, and you can see it because I've got children, right? So, I see what their education is now. When I was at school, they taught us very, very basic computer coding skills. Right, very basic. It was like learn how to make blink…blinking lights. Come on the screen or…or how to write a very basic video game script like…it was all for fun and there was never any link between that and this is something you could use in your life for a job when you get old or anything like that. So it was just…There was something I did when I was quite young, like 8 or 9, and then I went to my high school and didn't touch computing. There was none of it in the curriculum, you know. Now I'm a bit older, but subsequent generations have probably had a similar experience to me.

**Interviewer** 22:19  
Mm hmm.

**UPU2** 22:30  
Whereas in other countries they've been educating people, you know, and teaching people the importance of this stuff. So although it's improved, I don't think it's improved fast enough and. So. So for me, going back to your original question, I think that is one of the biggest issues as to why the UK is vulnerable. The other reason is…is politics.

**Interviewer** 22:51  
Mm hmm.

**UPU2** 22:56  
So you know. The United Kingdom operates certain policies and certain activities which puts itself into a global faction. Yeah. You know of other countries and you know that, see the world and how the world should be run a certain way. But the reality is there are plenty of other countries around the world that don't see the world in the same way.

**Interviewer** 23:11  
Mm hmm.

**UPU2** 23:29  
And added to that, you have the historical legacy of the United Kingdom, which you know, if you are born into the UK as a indigenous well, that's not the right word, but if you if you're born into the UK as a white British individual, sort of brought up on this diet of oh, how Great Britain is, aren't we? Aren't we good, right?

**Interviewer** 23:55  
Mm hmm.

**UPU2** 23:56  
But that's not how people that are in former colonies of the British Empire necessarily view us. You know, the people of India look at the history of the British Empire in India and say we utterly pillaged and stole everything that that country had on offer and we destroyed their economy. So. So it's that legacy plus you know, so that that creates a political tension in the world, which means that for a lot of people, we're not the good guys. And so they are going to have a pop at us and they are going to go after us for that reason. And we, when we sort of sit around scratching our heads as if to say well…Why? Why? Why are we being attacked? It's 'cause. They're, you know, they. But it's because not everybody sees the world the way the world's not everybody sees the world the way that Nigel Farage and Boris Johnson do.

**Interviewer** 24:59  
Hmm. Yeah, OK. OK. So it's like UK is trying to that put some policies you have to like, like you said, to put yourself in this, this global trend, but not every country sees the world or the cyber world the same way as UK. So some policy might not be that practical.

**UPU2** 25:25  
Yeah, that's an issue as well. So so. The best thing the UK could do now is to really focus its energy and efforts on being like a global leader around cybersecurity, both in terms of, you know, developing the technology, but also, you know, frameworks and like the rules, you know, because the internet's a bit like a bit like the Wild West in America. You know, you you it's it's a lawless place. You know, and there's opportunity there, but we've we've, yeah, there's opportunity for the UK to play a role, but we. We, we struggle, we struggle.

**Interviewer** 26:12  
OK. And let's go to section C. So for Section B was, uh, section B was like the general question, and section C will be the cyber defence strategy related question. So the first question is…As you know, like what are the overall cybersecurity plan of the UK Government and how do you evaluate them? But I think that you just mentioned that. You just talked about it a bit. Mm hmm.

**UPU2** 26:45  
So yeah, I mean so, so the, I mean essentially the UK cyber strategy, I…I haven't haven't seen the documents recently, but they, you know essentially it's a it's about making the UK somewhere that is safe that the economy thrives. That, you know that the online world is readily available for…for commerce and for…for…for good and for benefit. But also you know it's about recognising the threats that exist, that are risks to our economy risks to our way of life risks to our, you know, citizens, et cetera. And so you know, now we are starting to you know, put more detail around our the ways in which we…we, you know, we protect. You know, we protect our own, so. Yeah. I mean, there's been, there's been huge financial investment in this area. And you have. You know you have. That that, you know it's…it's not, it's not. It's not wrong to say that the UK has some pretty exceptional capability when it comes to defending its interests in a cyber, you know. I am not privy to or aware of any kind of covert operations that go on, but I'm sure they're going on. I'm sure we're probably as a nation now doing to our opponents what they're doing to it, or they have been doing to us, it just might be that what we do is more discriminatory. So the way I kind of think it works in places like China is you've got these huge groups of individuals. Huge group. You know, offices of buildings, you know that are part of the Chinese military or whatever they happen to be. And basically they come in and they just have a pop and have a go at whatever they want to have a go at. And it's all very.

**Interviewer** 29:11  
Mm hmm.

**UPU2** 29:14  
You know, it's all sometimes they get directed with specific objectives, but other times it's just go out there and see what you can do. Whereas I think the UK, the cyber defence strategy is probably a lot more targeted. It's it'll be like, right, you know, for argument's sake, let's try and infiltrate computer networks in Iran or Russia or whatever it happens to be.

**Interviewer** 29:37  
Mm hmm mm.

**UPU2** 29:41  
But that's just, that's just me guessing that's…that's…that's not based on any personal experiences I've had.

**Interviewer** 29:48  
Hmm. OK, that's fine. OK. Then question number 2 and three, I will just ask you like you, because I think they they can be answered together. So number 2 is about the cyber threat precaution. Yeah. So what do you think about the current cyber threat precaution strategy? And like it's like, are they good enough or how can they be improved?

**UPU2** 30:22  
So. I mean. It it kind of goes back again to this issue of cyber becomes…It only becomes…it only becomes like the focus of people's attention usually when things go wrong. You know what I can tell you from dealing with people in industry that work, work in this world, you know, is that they they really struggle to be taken seriously until there's a problem. So they will say…

**Interviewer** 31:02  
Mm hmm.

**UPU2** 31:04  
They will forecast and they will predict issues and risks and they'll say we need to do something about this. We'll need to do something about that. But very often in a business context, commercial interests are prioritised, right? Yeah. It comes first. So until there's a problem and then everyone's like, alright, we need to throw some resources and money at that. So I think the same can be said about government overall government strategy. The government has got. I mean we've got a new government now and they've got a million and one things that they need to solve. So, part of what they need to look at will be cyber defence and cyber strategy and all the rest of it. But but I wouldn't be surprised if it's something that isn't exactly the burning issue of the day, because the burning issues of the day will be getting the economy to grow. Reducing the..the migrant issue that, you know, is currently unfolding in the UK and…and other things that the voters have said they want the government to prioritise, right? So. So I…I think that's the problem that we have. And dare I say that in other parts of the world they don't have this problem is…is that you you want? You need to keep cyber in the in the headlights and keep it there. You need to get it there and then keep it there. But that's very hard to do and the and the way to do that really is just through constant education at all levels.

**Interviewer** 32:29  
Mm hmm.

**UPU2** 32:39  
And you know just. Yes, it's. I think it's it would take, it'd take it was taking us several generations to get to where we are today and you know, but we probably need more time to get to a better place. One thing I would say that we're good at though is is that people, there's a lot of people that are really passionate about this subject, really passionate about cybersecurity, information security networks, computers, all that stuff, right? Tonne of people that are really passionate about it. And they and those people work in industry, they work in government positions and because they're passionate about it, they actually are quite effective at identifying vulnerabilities or…or spotting new trends, or coming up with new technology. That that, that changes the game, you know, so that's…that's an advantage that we as a nation have, the UK has.

**Interviewer** 33:49  
Mm hmm.

**UPU2** 33:51  
Which I don't know. I've never lived in those other countries, but I I don't. You don't hear so much about that, you know, like when you go on the global stage for cybersecurity, this there may be a number of reasons for this, but you…you don't get to hear from the absolute celebrities of cybersecurity from Russia or from China or from wherever else in the world you want to pick, and I don't know why that is but, but that might be something to do with our systems are different. You know, it's just the, you know, our political and our societal systems are different, which means our system, for all its faults, gives people the space to be creative. Choose what they want to do and choose to be passionate, and when you volunteer to do something and you are passionate about it, you tend to be one of the better ones at it, rather than somebody who's kind of conscripted into doing it. See the difference? So I think that's yeah.

**Interviewer** 34:57  
OK. And then so when you talk about the education, I think we can jump to question number 9. So do you know any of the current governmental plans for the cybersecurity education?

**UPU2** 35:15  
No, it's a short answer. No idea, no. What I can say is that in…at school level. They've just made changes at school level that says that all schools have to understand cybersecurity. So that's the teachers and the right. So the staff at schools have to understand their responsibilities and have to have training on cybersecurity to keep, to keep children and the and the schools safe from hacking and all that.

**Interviewer** 35:38  
Mm hmm.

**UPU2** 35:54  
And I know that the curriculum now children learn, you know, coding and ICT related topics where it gets where unfortunately it goes wrong is when they get to secondary school, it's not a priority subject. Let's talk. So that in terms of government education, in that sense of educating the whole society, that's an issue. Then, but then what you've got if you skip a level and you get to university, you've got some interesting things. So obviously we've got loads of universities in the country that are offering various cybersecurity degrees, but all different topics, right? That's great.

**Interviewer** 36:42  
Mm hmm.

**UPU2** 36:45  
But in addition to that, what the government has also done is it's it sponsored organisations which have created what they call boot camps. So boot camps are for people that haven't been to university, but maybe have had a career doing something else and they want to get into cybersecurity. So there are pathways now for those people to get into cybersecurity as well, because we're trying to get as many people as we can into the industry. So that we can we can meet the demand that's there. And so that's…that's a good thing. That's an innovative thing that the government has, it's not…it's not created these courses but it's…it's given the funding to organisations that have been created these courses.

**Interviewer** 37:19  
Mm hmm mm hmm mm. OK. Yeah, that's…that's good. And what do you suggest to improve this education on the…the…how do you say, the elementary level education for cybersecurity?

**UPU2** 37:49  
So traditionally in the..the absolute most important subjects have always been English which is learning to read and write literacy. Mathematics and science, right? Those 3 subjects have always been the…the most important subjects. And and and what they need to do is add computer science to that. Because the world has changed, and if we if we, you know, when I went to school, computer science, computing, whatever you wanted to call it, it was something you did as a hobby. No one ever thought you're gonna do that for a job. Not in my generation, really. It wasn't. It wasn't pushed on us. But if you think about how far technology has come just in your…What you what decade were you born? I won't ask you how old you are, but what decade were you born?

**Interviewer** 38:57  
What decade?

**UPU2** 38:59  
Yeah.

**Interviewer** 39:02  
Like 1990 ish.

**UPU2** 39:06  
Right 1990s. OK. So when you were born, right, we were still using cassette tapes. And if you wanted to watch a movie, you had to go to a video store and rent it for, like, a few pounds or whatever the…the currency was. And then take it home and put the tape into a machine. It was analogue technology, right? And you think, like, now if you wanted to watch your most favourite movie in the world, you could just within 5 minutes have it on your phone that you've got in your pocket, right? now.

**Interviewer** 39:19  
Yeah, yeah, yeah, that's big change. Yeah. Mm hmm.

**UPU2** 39:39  
But or or for example. Yeah, it's a big change, isn't it? Or you know for me, when I was a young boy, if I needed to go to the doctors, I would have to get the bus into the local town, go up to the reception desk, request an appointment, come back at another time or maybe phone through. Now I can get all my medical stuff done by filling out a form on my iPad and get the answers within an hour. Oh, yeah, you know. Oh, you don't need to come in. We just renewed your medication or whatever it happens to be, you know, technology, our lives as human beings is very much fused with information technology. And you think of how much that's changed since the 90s, right. And then think, well, how much more is it going to change in the next 20 years, 30 years, 40 years? So, yeah. The government needs to put information technology at the heart of school curriculum. You know, it should be. It should be like a a mandatory thing that you do up until the age of 16 or 18 even.  
Yeah, I mean. Yeah, that's probably the best thing they can do.

**Interviewer** 41:01  
Yeah, OK. I agree with you. Yeah, like the everything is changing. So the education material and whatever you we have, we also have to keep up pace with that the the changing world. OK then. Let's move on to question number 4 and 5 because before we were talking about the precaution, now how about, you know when you are dealing with the ongoing cyberattack? And So what is the what are the strategies that you know that how do we react? How do we respond?

**UPU2** 41:42  
So there's there's lots of different…different frameworks, different organisations that you know. But in simple terms, you know the…the formula that is followed is you…you contain an incident. You eradicate or you work out what's causing it and you eradicate the problem. Then you restore your systems to how it should have been before and then…And then post that you kind of…You look at why it went wrong and make sure that you've patched the issues so that it can't happen again, right? So in basic terms, that's how it should work.

**Interviewer** 42:25  
Mm hmm mm hmm.  
Mm.

**UPU2** 42:32  
You can.  
You can well, it depends on what level of attack you're dealing with, right? If you're dealing with like an attack that's hit some business, that's as far as it will go. You're talking about a major attack on a major government department or part of the, you know, the government, you know, or some major, major, major organisation that's, you know, really. Either significant in terms of its brand or in terms of the revenue that it brings to the economy, well then, you're gonna try and go further, and you're gonna try and identify who's done this and why they've done it and how they've done it and all those sorts of things, right, so.

**Interviewer** 43:11  
Mm hmm mm hmm mm.

**UPU2** 43:15  
You know, I was a police officer in a territorial area, right? I didn't have to deal with that many crimes of hacking because they didn't happen that much on our on our area, but when they did, it was to small businesses and we would just effectively say, right, first and foremost, get control of your system. Get them out. Restore yourself back to where you need to be. Make sure that this can't happen again tomorrow. In the same way, because you've…you've identified how it happened, etcetera, and that would be that. And then separate to that, my job was not to deal with that side of it. My job was to then say, right, who's done this? How have they done it? Why have they done it?

**Interviewer** 43:49  
Mm hmm.

**UPU2** 44:03  
Oh, I've lost you again. And she'll come back in.

**Interviewer** 45:23  
Hi, I'm so sorry about that. I don't know why I think it's my that the Internet, the Wi-Fi in my in my house. OK. So let me just.

**UPU2** 45:28  
Don't worry, don't worry.

**Interviewer** 45:34  
Turn on the recording again. Oh, I think it's it's on.

**UPU2** 45:40  
It's still going, is it?

**Interviewer** 45:41  
Yeah, let let me check. Yeah, OK. Yes.  
So sorry so. So we were, yeah, we were talking about the the ongoing cyberattacks. So you were I think you were you were saying cause during that time they…they weren't many hacking, but when he when he did it just small business and then how you told them what to do with that after that. And then…

**UPU2** 46:15  
Yeah, exactly that. So it's so it so so my, my role within the police would not be to do that. So so within the UK, we have something called the NCSC, which I'm sure you are familiar with, right?

**Interviewer** 46:27  
Yeah, NCSC.

**UPU2** 46:29  
Yeah. And also we have the National Crime Agency. So the National Crime Agency has the best law enforcement capability to investigate and prosecute people that have committed crimes that. Hacking would be a crime in certain circumstances, right? So I didn't work for a national organisation. I worked for a local police force, so the level of crimes that we would deal with would be not that sophisticated. But we did get some. Yes, so so my…my job was always was to like, you know, listen to what the allegations were and try to test them based on the evidence that was available to me. So you know, one case I dealt with was a case of alleged industrial espionage. So it was a company that was developing a very profitable piece of technology. If they could have ever got it to work. I don't know if they ever did, but…but had they had they got it to work, it would have been, you know, very, very profitable as a, as a piece of technology. They…they suspected that a competitor was trying to sabotage them. And that they've done this by hacking into their systems, et cetera, et cetera. So we had a look at that for them. And. Although that did lead to an arrest and interviews. It ultimately didn't lead to any prosecutions because we didn't have sufficient evidence to…to prosecute.

**Interviewer** 48:06  
Mm hmm.

**UPU2** 48:06  
But so yeah, so in terms of, yeah, cyber incident response, I I don't do that. I never have done. We would just give generic advice on that. It really just depends on the nature of the organisation as to what they do, you know. You know big organ…I mean, now I work some of my clients are huge organisations that are part of what we call a critical national infrastructure. And so they have. They employ instant response teams, but they also have insurance policies which mean that if it goes…ever goes really wrong for them, then the insurers would bring more resources to help recover and…and…and all the rest of it. So. Yeah.

**Interviewer** 48:59  
OK. Yeah. So it depends on which company, which organisation and what…what source you are using? Some of them they have. They so and then in your opinion, what would you suggest them like? They have their built-in cybersecurity personnel or they outsource to the third party?

**UPU2** 49:30  
So. I think that in terms of cost effectiveness, it's better to outsource a lot of the time. And also. Depending on who you go with, you might get better expertise through outsourcing. But it's it's really. So that's a really difficult question to to to answer because it just depends on each organisation and its needs.

**Interviewer** 51:09  
Sorry again. I'm so sorry. I don't know. I don't know what happened, but I checked my Wi-Fi. It looks good right now. I don't know why it just dropped off. OK, so.

**UPU2** 51:11  
Don't worry. So I I I don't you missed anything. I I was just saying it it really just depends on on the individual organisation or company. I mean you know for for for UK government they obviously can't really outsource because they need to be able to trust the people. But for industry, I mean, there's some big, big players already in the industry that kind of provide those, those…those. Hmm. Those things and the…the other good thing is there's a lot of, there's a lot of opportunity to share lessons in the industry. The very open industry in terms of talking people get to learn what happens in, in things and then learn from that so that they can adapt those things in their own organisations.

**Interviewer** 52:19  
Mm hmm. OK. Then let's move on to question number 6 and 7. So it's about the the post cyberattacks. And do you know any of the strategy about post cyber attacks and how do you evaluate them?

**UPU2** 52:27  
Yeah. Yeah. So again, this is not something I've been directly involved with. But yeah, I mean. Essentially, it's there. There is a lot of emphasis placed on learning the lessons and learning quickly. And as I said, there is a lot of proactive knowledge sharing in in the industry and in, in across government as well. So that when things happen, people can react to it quickly. So you know, for example the, the, the recent. Ticketmaster breach. I'm not sure we all know exactly how that's been caused.  
But as soon as the detail is, is, is understood that will get shared out and and within hours, organisations that can will have looked at it, looked at what happened, assessed it against their own controls and vulnerabilities and gone, oh, we've got the same issue we need to we need to patch this or we need to change this or we need to do this. And it'll get done. So in that sense that, you know that's that's a good thing that I think happens in the UK and and and the US, I mean in English speaking countries, there's a lot of crossover you know so UK, Canada, United States, Australia, New Zealand, you know the Community chat talks you know.

**Interviewer** 53:50  
Mm hmm mm hmm

**UPU2** 54:14  
So.

**Interviewer** 54:15  
OK. So it's also kind of like international cooperations on that, OK.

**UPU2** 54:20  
Yeah, yeah, yeah.

**Interviewer** 54:24  
OK. And let's go to question number 8. So how do you describe the the awareness of the cybersecurity among the general public?

**UPU2** 54:37  
It's definitely more. It's definitely more understood now than it was ten years ago, but I still don't think the average person understands the gravity of cybersecurity, like the importance of cybersecurity. Really. Because they've never had an experience as a result of a cyber attack that has directly affected them and their way of life. But you know, if if if we as a country, say found ourselves with our relationships with other parts of the world severely, you know, even further deteriorated than what they are today. And you know they successfully hacked into our power supplies or into our food supply chains or people would soon get it, right? It wouldn't. It wouldn't take much, you know, to if you think about like COVID right? COVID came along and…Were you? Were you living in the UK when that happened, or were you in Taiwan or?

**Interviewer** 55:58  
No, I was in Taiwan, yeah.

**UPU2** 56:00  
Right. I'm not sure how it was for you, but here. We had shortages of everything.  
But you…you couldn't. You could not go to the supermarket and buy a a packet of pasta. You couldn't get it. It was, it was like. The closest we've ever been in this country to how things were in the Second World War when we had rationing, you know, you go to. I was a police officer then and I would finish work and I would have to and we were all like it had to limit what we were doing. But I would go to the supermarket to buy food for my family and I couldn't find anything. No bread. No this. No that. That that COVID did that, but a successful cyberattack, or coordinated cyber attacks could achieve, maybe not on the same scale. In times of warfare, it could. But in in in times of peace, so-called peace, you could certainly disrupt, y ou know, vital supply chains using cyberattacks, and then people would know, but generally speaking, I think that the awareness and appreciation in the United Kingdom is not where it needs to be. It needs. There needs to be a, a, a raising of the of people's awareness.

**Interviewer** 57:10  
Mm hmm. OK, so it's so people, they generally they don't really have this sense until they realise their lives are involved with, are affected by that.

**UPU2** 57:39  
Yeah, exactly that. So if you said, you know most people. I mean. If, if, when you talk about hacking and sort of that most people will think about crimes, they won't think about actual the big stuff, they'll be thinking more like…somebody stealing your bank details, somebody who's conned your auntie into giving away 10s of thousands of pounds because they thought that they were going to get married to somebody that doesn't exist and you know all these types of things. That's what. That's what's in people's minds and imaginations than thinking about, you know, people that are hacking into businesses and net systems that could then actually have a real impact on.

**Interviewer** 58:32  
Mm hmm mm hmm. OK. And.  
So that question number 10 is I think you also talk about it before. So what is what are the current governmental cultivation plans to attract the future cybersecurity talents?

**UPU2** 58:55  
So what the what? The government's trying to do? I know this for a fact is the government is trying to create very, very clear pathways. So that if you're a young person. Or maybe not a young person. You're a slightly older person, but you have a a desire to get into cyber security. You'll be able to go on government websites and see really clearly the path from A to B, right? How you get there, because at the moment it's a bit unclear, and so they want to they're creating a system where so, so, for example. Like in this country, if you think about doctors, right, medicine, there's a real clear pathway for a young person that says I want to be a doctor to get into being a doctor. It's really prescribed even to the level that each year, when they, the universities release their cases, they know exactly how many places to give to students based on the number of vacancies in the NHS. Projected vacancies. So the whole thing is intelligently worked out and that's what the government is trying to do now with cybersecurity. But it's gonna take them, I think 10 or 15 years, at least to get there. If they ever get there.

**Interviewer** 1:00:23  
OK, but it's. But still in the right track the right direction. OK, OK, that's good.

**UPU2** 1:00:29  
Yeah, yeah, it's positive. It's positive. Yeah.

**Interviewer** 1:00:34 58;39  
OK. So how do you what do you suggest…suggest if for this kind of plan. I mean if you said it's going to take like 10 or to 15 years to get there, but you know So what can they do to make it quicker or to?

**UPU2** 1:00:56  
Accelerator. Yeah. Yeah. To accelerate it, yeah.

**Interviewer** 1:01:00  
Yeah, yeah.

**UPU2** 1:01:04  
Well, that's a really good question. I…I think they should….Well, I think that they…they need to have like a route like a an entire review of their whole strategy. Understand what it is that they want to achieve, what are their big strategic aims. And how they're going to achieve those strategic aims and then work backwards from that. But I think it will look like…Some of the things we've talked about how, you know, as a nation we should be championing and promoting information security and information technology skills and knowledge from a very early age consistently so that when…when you get each crop, a new generation that gets between 16 and 18 years old, a significant number of those people, more than what we have today, are heading towards careers that involve cybersecurity, keeping the United Kingdom safe, allowing business to thrive and flourish. And all the rest of it but within…within that context. Yeah, it's not uneasy. It's not uneasy thing for them to have to do, but I think it it requires big, ambitious thinking, which I don't think any government up to now has done because, you know, the problem with all governments is they have a lot of problems to deal with and they have to kind of put them in order. Sometimes you might grab something like cybersecurity say, right. We're going to make this a priority and put it here. And then all of a sudden, the global pandemic comes along, and you have to go, oh, take that out. We're dealing with that now.

**Interviewer** 1:02:34  
Mm hmm.

**UPU2** 1:03:03  
So I get it, I get it. It's it's, you know. You know, in an ideal world. We'd all stop disagreeing with each other. We'd all stop fighting each other for resources, and we'd work out how we can, you know, live on this planet and not have to compete with one another.  
And there's a real and there's a real gap, right? When you think about everything else we do, right? You think, like, the United Nations we have, we have organisations, international organisations on things like poverty, on hunger on, you know, peace and diplomacy and war and, you know, all these things right that we cooperate in a space exploration, we cooperate internationally. We're not really that good at cooperating internationally when it comes to technology and information security, you know, and we, you know, and…and actually maybe the way to go forward would be for the UK to take a bit of a leading voice and say, you know what, we've all misbehaved in the past. We've all done things to each other that we shouldn't be proud of, but let's stop all of that and let's work together as a family of nations, right? To kind of create a world where we can all coexist and…and work in a mutually beneficial way via information security and in in our online. Because what if you start doing that? If you bring state actors on board, then all you're left with is criminal gangs. And criminal gangs will…will always cause harm. But they can never have the impact and the reach that's that nation states can.

**Interviewer** 1:04:45  
Mm hmm mm hmm.

**UPU2** 1:04:52  
So you would make, you would make a, you know, you'd. So that's what I would like to see. I would like to see the world coming together to work on these issues rather than, you know, bashing against it, yeah, yeah.

**Interviewer** 1:05:11  
OK. Yeah. But that, that that's, I don't know. I think that that would take a lot of energy and too a lot of effort to reach that point.

**UPU2** 1:05:23  
Yeah, I think you're right.

**Interviewer** 1:05:41  
Yeah. Yeah. OK, let's go to section D. Section D are just some question about public private partnerships. So the first one is what do you think of the idea of public private partnerships on this cybersecurity? Do they really help to improve the cybersecurity?

**UPU2** 1:05:49  
Do you mean we're private organisations or companies work with the public sector?

**Interviewer** 1:05:57  
Yeah, kind of like the public sectors like governmental institution and then work with the cybersecurity firms or cybersecurity providers.

**UPU2** 1:06:06  
It it does work and the reason it works is because you, if you can tap into the private sector, you…you have a choice of products. You have a choice of expertise, individuals. So you can…you can pick what's best to achieve your objective. If you…if you say, as a public sector organisation, we're not going to go outside and work with in industry, then you're limited to the skills and the talent of the people you've got, which is small. Can never be better than what's out there.

**Interviewer** 1:06:51  
Mm hmm.

**UPU2** 1:06:52  
And and there should be this constant like crossing backwards and forwards between the two worlds. So I go and work over here in the private sector. Get all this experience. Then I take that and work in the public sector for a bit and then I come back and do this. You know, there needs to be that cross poll. That's the most effective way. The risks are private sector have different aims and objectives to public, you know. Ultimately, they're rooted in commercial aims and objectives, which might not always align with what the government needs in a given set of circumstances.

**Interviewer** 1:07:31  
Mm hmm.

**UPU2** 1:07:34  
There's some pretty bad examples of public and private working together. In…it not maybe not in information security, but certainly in ICT. So if…you if you take the, are you familiar with the post office scandal that that that we've had?

**Interviewer** 1:07:45  
No, not really.

**UPU2** 1:07:52  
So there's a huge national scandal that's currently the government's had to apologise for. And they're having to pay out millions of pounds in in compensation. And it's because in the UK, the post office, which are part government, part private, partners with Fujitsu who are a massive ICT and cybersecurity firm to create a system to to to operate their post offices or the system had flaws in it. And So what it was telling the post office was that all their post office workers were stealing money. They weren't. It's the system was wrong. So what the post office did was that they they they had all these post office workers prosecuted and sent to jail, even though they've done nothing wrong.

**Interviewer** 1:08:34  
Mm hmm mm hmm.

**UPU2** 1:08:55  
So that's all come to light and it's massively undermined the ability of government to trust private sector. And who's responsible? Is it government? Is it the company? Is it Fujitsu's fault? Is it? Is it the government's fault? So. So there are risks associated with these partnerships. But I, but ultimately I know from having worked in a public sector organisation, is that you can't, you can't achieve everything with within the means and the resources you have private sector brings so much more to the to the table.

**Interviewer** 1:09:29  
OK then. How can they? Because you you just mentioned this kind of risk that the trust and then how can they manage to do it? What do you suggest?

**UPU2** 1:09:52  
So there. Well, So what they try and do is that they have governance and accountability. So. So in an ideal world, you agree a contract you work together, you make sure that you vet the people, you that you're gonna work with so that you're not taking on security risks. So you make sure that the back, you look into the backgrounds of the people that are working at the private company to make sure there's nobody there that's you know, of concern. Once you're happy with that, You…you then, you know, you agree like this is how it's going to work. This is what you're going to deliver. This is really clear. But then this is how we're going to manage and look at the accountability.

**Interviewer** 1:10:43  
Mm hmm.

**UPU2** 1:10:43  
So we're going to measure that. This is what you told us you were going to deliver, and we're going to check that…That's what you're delivering every so often.  
And measure it to make sure that we're satisfied and that if we're not that there's that you're held accountable. What happens all too often in the UK is that UK government organisations get into agreements with the private sector where they they don't do any diligence around how they form those relationships, the contracts and all the rest of it. And so, these private organisations will come in and often they'll do a bad job. And there's no accountability because the, the, the way that the contract was negotiated was really badly. And the reason for that is because if I'm, imagine, say I'm a big consulting company, like I won't mention names, but let's say I'm a big consulting company, I'm going to have lots of lawyers paid lots of money. Versus a small government department that might have access to one lawyer who doesn't get paid an awful lot.

**Interviewer** 1:11:49  
Mm hmm.

**UPU2** 1:11:50  
So the effort they put into to make this relationship happen is not enough. Like time and time and time again, the government gets done over basically, by private sector. So there's definitely something around that I would say. Just making sure that you you do your due diligence around. You know, terms of reference terms of term, rules of engagement and that there's clear accountability. If it goes wrong, it's…it's you, not us or it's…it's both us but it's you.

**Interviewer** 1:12:19  
OK, good. OK. And then if they work together like, what do you think the the public sectors can contribute to this partnership and what are the contribution from also from the the private sectors to…to these partnerships?

**UPU2** 1:12:57  
Well, so the contribution from the public sector, I suppose is is the fact that they are.  
They are…they are working on behalf of the people and so it's in the public interest and. Therefore, they bring legitimacy to these relationships and and an important purpose. I suppose.

**Interviewer** 1:13:33  
Mm hmm.

**UPU2** 1:13:34  
They. You know, if we're talking about cybersecurity partnerships in in bigger terms, I suppose may have influence, right? They have government governmental influence. So you know if if if my…my former organisation were partnering with industry to trial some kind of new cybersecurity method or technique. You know, we would have reach into government and we would be able to demonstrate that this is a good thing for not just us, but for other organisations, so we can, you know, you can have a soft influence on UK government strategy etc. That's what they bring.

**Interviewer** 1:14:20  
Mm hmm mm hmm.

**UPU2** 1:14:23  
And sometimes, you know, I guess.  
You know, when things are really serious, they can bring that kind of influence and decision making to the partnership. What private sector brings is…just that. Potentially more infinite resources and and diversity of experience in, you know, workforce and things like that. So it it they're just if you work with industry, you're they're likely to be more agile and and more flexible in dealing with a problem. So if you put, if you put just the government department on solving a cyber security issue, they're going to move at a certain pace. They're going to think only in a certain way they're only going to have limited resources to do things a certain way. If you add a private sector partner into that. They bring new ways of thinking, much more adaptability. They can work quicker, they can work, you know, harder, so many things. So. So I think there's definitely benefit for these options.

**Interviewer** 1:15:40  
Mm hmm. OK. And and do you are you familiar with the current cooperation mechanism. Do you know any of the the examples of they work together to deal with this cyberattack or cybersecurity issue?

**UPU2** 1:16:03  
I I mean, I can't give you any very specific examples, but for example I would say that. If you talk about BAE Systems, right? BAE Systems, huge defence company, absolutely vital part key partners, strategic partner with the the UK government. Because in addition to supplying missiles and warships and things like that, they're also heavily in the cybersecurity space. So you know they are a private company, but they have a special relationship with the UK government. So if you…My my advice, if you, I can't, I can't give you any more tangible information, but my advice to you would be that would be a good direction to look in.

**Interviewer** 1:16:56  
Uh, huh. OK, the BAE system with the government.

**UPU2** 1:16:58  
BAE Systems? Yeah. Yeah. Because they are. You know, they're they're kind of the. Yeah, I mean they, they are. They're huge and they they are. They're cyber division is getting bigger and bigger and bigger.

**Interviewer** 1:17:17  
OK. Last question for you. And So what would you suggest for the future partnerships between like what can they do to improve or to make it better for these partnerships?

**UPU2** 1:17:36  
Do you mean? What? What can government and industry do to make partnerships in general better?

**Interviewer** 1:17:40  
Yes.

**UPU2** 1:17:55  
I’m not sure. I I think there's…I think one of the biggest problems in the UK is that there's not. Everything's disjointed. Nothing's coordinated. And so. Maybe the the answer would be some kind of a forum where industry and government come together and that forum or that organisation becomes the absolute go to place for everything. The moment in in cyber security, you know, there are many, many different regulations, standards, best practises organisations that you can become a member of. You know, it's just so much. It's such a cluttered, crowded landscape or…and none of them are the single most authoritative source of what's good in cybersecurity. So maybe what? What the government needs to do, and I don't. I don't know if they do this already, but it is in conjunction with some really big strategic partners. Create a space, an organisation, whatever you want to call it, where government and industry can come together. And in that organisation, that is where not only are relationships forged, commissioned and then that partnerships go forward, but also it's a…a forum where people learn and share ideas.

**Interviewer** 1:19:47  
Mm hmm mm hmm.

**UPU2** 1:19:50  
So that it all becomes connected, because at the moment you know. There'll be a complete disconnect. Let's say you take. I don't know the Ministry of Culture, Media and Sport, right? Just taking a random department from the government, OK. They may well have some very relevant cybersecurity issues that they need dealing with.  
But I can almost bet that they're not talking to the Ministry of Defence and their partners, who might have a solution for them. So they're working like almost against one another, or in random ways, rather than everybody being together, working together and going, right?

**Interviewer** 1:20:32  
Mm hmm.

**UPU2** 1:20:33  
We're over here. We've got this problem, but we need this solution and then the whole community of government agencies goes, ah, well, we did this for this or you want to talk to these people or whatever. Do you see what I mean?

**Interviewer** 1:20:45  
Mm hmm.  
Mm hmm. Yes, it's kinda like information sharing platform, you know, OK.

**UPU2** 1:20:52  
Yeah. Yeah. But, but yeah, that would be like on one level that would be it. It would be an information sharing platform, but also somewhere that would be the the authoritative voice within cybersecurity. So you go to this organisation for guidance on everything that's to do with cybersecurity rather than having 15 different sources of, you know, oh, that's how you do this. And that's how you do that. Or. But then there's that version. There's. That's how it is currently, you know.

**Interviewer** 1:21:26  
Mm hmm. OK, OK. So yeah, I think that's a good idea like current.  
Current for forums there, there are too many platforms so everything is really disorganised. You see things here everywhere and you don't know which one you can follow.

**UPU2** 1:21:47  
Yeah, exactly. So you know you for example, you've got ISC squared. Go to those ISC squared. With ISC squared, you know you can access training, you can access qualifications. But then you've got the SANS Institute.And then when you talk about regulations, you've got American standards, you've got UK standards, you've got EU standards, you've got, you know, it's like it's just it's so cluttered. So messy and it would be like, you know what, you know, UK industry, right, this is what we're gonna do. We create the forum, everybody comes together into this space. If you need, you know. And so I'm sat in any government department. I've got a cyber issue and I they go well. The first thing you need to do is go to the forum. And the forum will guide you and point you in the right direction of how you solve your problem. And they will say you know, OK, you need to partner with industry. Here are 10 providers that we've already vetted because they're part of the forum. Yeah, we've already checked that they're suitable. They're part of the forum. So now you can do a tendering process and decide which one of the ten that you're going to go with.

**Interviewer** 1:23:04  
Mm hmm. OK.  
Right. OK. Then I think that's it. Thank you so much. Yeah. Yeah. Let me just let me press stop.

**UPU2** 1:23:18  
OK, no problem.