**Interviewer** 0:14  
OK, so I think we are recording right now.

**UPU1** 0:18  
Yes, it says somewhere.

**Interviewer** 0:19  
Yes, yes, it's recording right now.  
OK.  
So then let's get started.  
So, uh, I'm going to start from section A for the basic information. Yeah.

**UPU1** 0:33  
Yes, please.

**Interviewer** 0:34  
So uh, section A uh, the first question, I will put you in public sector because you.

**UPU1** 0:40  
That's.

**Interviewer** 0:41  
Yeah. So you've been working in a the [the name of a police department].  
Yeah. And then the second question is what unit do you work for right now?

**UPU1** 0:51  
So I work for a cyber crime unit.

**Interviewer** 0:54  
Uh-huh.  
OK, in.  
Yeah, in [the name of a police-led cybersecurity awareness programme], right?

**UPU1** 0:59  
In [the name of a police-led cybersecurity awareness programme] yeah so in [the name of a police-led cybersecurity awareness programme] is an internal unit within the cyber crime unit.  
So the way that the unit is divided is there's an investigation arm, which is in my history. And then [the name of a police-led cybersecurity awareness programme] is to protect and prevent, which is the education arm.

**Interviewer** 1:18  
OK. And the third question is, umm, how long have you been working for this unit?

**UPU1** 1:25  
Eight years.

**Interviewer** 1:27  
Eight years. So that's that's really a long time.  
And then what position do you hold within this unit?

**UPU1** 1:33  
I'm a senior detective.

**Interviewer** 1:35  
Senior detective and the last question and what are your main responsibilities?

**UPU1** 1:41  
My main responsibilities are education. So I do education to private industry, residents and…and also international clients as well. We also give protect notifications and we also do prevent work with schools, children, parents, etc.

**Interviewer** 2:03  
Umm. OK. Umm. Then also do you also provide training to the police officers, maybe?

**UPU1** 2:13  
Yes, yes, we do. So all all, all new starters…um, when the when they are on boarded, they will be given cybersecurity training as well.

**Interviewer** 2:23  
So then that's go to section B. So section B is for the…the comprehensive, general cybersecurity questions, section B.

**UPU1** 2:34  
That.  
Yep.

**Interviewer** 2:37  
Yeah. OK. So the first question is, umm, what are the major cyberattacks in the UK and what are the models operandi and you can also give some examples.

**UPU1** 2:50  
OK.  
So in terms of cyberattacks, the highest percentage is still seen around phishing and spear phishing and used very much as a pivoting point for then further types of criminal…criminality. So ransomware, deployment of malware, uh, extortions, blackmails, sex extortions. So quite a subjective question because it depends on the motivations of the attacker and who obviously the attackers are. If they're organised criminal gangs or state actors, et cetera. So but we are still seeing a little I think the last stack that I saw was the 83% of all cyberattacks in the UK start with phishing.

**Interviewer** 3:36  
I'm sorry, I think I lost you for the the the last minute.  
Can you say that again? Start from, yeah.

**UPU1** 3:43  
OK. What was the last thing you heard? Sorry.

**Interviewer** 3:48  
Uh, like you started from…if you say if they're organised criminal gangs or state actors and then.

**UPU1** 3:57  
Yep. Uh. And then I went on to say that the the last statistic that I saw was that 83% of all reported crimes start with phishing.

**Interviewer** 4:07  
OK. OK then. So because you mentioned about, it's depends on their motivations.  
So can you like, give some example of like different motivation then they might commit different kinds of? Yeah.

**UPU1** 4:23  
Yet. Absolutely. So, and if it's like so, excuse me, it was a financial motivation.  
We've seen phishing leading onto business email compromise. They then sit within that Business Network for up to three to six months, I'd say on average, understanding behaviours, syntax learning time frames around financial, uh, invoicing timelines, et cetera, um…before they then take over that account in order to do a mandate forward as an example. To try and get funds redirected to different bank accounts et cetera. So that's one motivation. You can get hacktivists again doing the same thing, but you know where to get a foothold onto the network and then to either do damage, et cetera. Steal data for other…other means with political motivations. So I think that they're two relatively good examples there that we have seen.

**Interviewer** 5:37  
OK, so the like the major 2 motivations will be financial gains and the other one is Political issue.

**UPU1** 5:45  
Yeah. I…I…I believe so, yeah.

**Interviewer** 5:47  
OK, yeah. And so then let's go to the…the question number 2.

**UPU1** 5:56  
Mm-hmm.

**Interviewer** 5:56  
And So what are the major targets of cyberattacks in the UK and also what are the reasons. I believe you just mentioned some of them the motivations, yeah.

**UPU1** 6:05  
Yeah. Again, a very subjective question. And you know, if you're, if you're starting to look at state actors attacking the UK, you're looking at critical national infrastructure. You are looking at the financial industry…uh, because these are the two areas are going to do the most harm.

**Interviewer** 6:25  
Mm-hmm.

**UPU1** 6:25  
Uh, if you're looking at organised criminal groups again, it could be any business sector, because what they are looking for again, it's financial gain. So you think you ransomware extortions, ransomware as a service. Uh, it…it could even be down to corporate espionage, if it is a competitor, the competitor. So we can see, be seeing denial of service in whichever iteration it wants to…to wear itself down to insider threat. And so yeah, quite subjective question.

**Interviewer** 7:04  
Umm. And then in your opinions, uh, do you think there will be some specific industry that will be easier than other industry to be targeted?

**UPU1** 7:18  
Umm, I wouldn't say industry specific. No. If you start looking at the size of organisations. So probably SME. I think SME are far more risk than larger organisations purely on the basis of their financial budget that they can put towards cybersecurity, um, as well as a lack in knowledge from these estimates, and so I feared they're probably more at risk than a larger organisation. But then they may well also sit in the same business sector as some of the larger organisations. So I wouldn't…I wouldn't be specific in regards to business sector and but I would go as far as budgetary constraints and organisational size. That would be my…my best opinion.

**Interviewer** 8:16  
OK, then I see and then let's go to question number 3. So what are the factors affecting the cybersecurity in the UK? And you can also give some examples.

**UPU1** 8:30  
OK. Uh again, I mean this…this is a large list of, obviously. I've written some notes for you. It's for to prepare myself.

**Interviewer** 8:40  
Ohh thank you so much.

**UPU1** 8:43  
No worries.  
I think for me, the first of these really is gonna be the cyber threat landscape. Uh, this is evolving at a significant pace. With that landscape of becomes your different level of threat actors. So we've got. So you've state actors, you are criminal gangs that we were spoken about hacktivists potentially inside of threat that you're inside of threat again can then be divided into a number of sub categories. So you can have your disgruntled employees or ex-employees. You're just gonna have human error, to be honest. So you're normally just human error, but I still was an insider threat. Uhm.  
The things that we need to…to really consider, um, again around that landscape and we're actually looking at the capabilities of our attackers. Um, you know your…your script kiddies aren't gonna be as sophisticated attackers with your current up against nation state. Particularly, you know, we are looking at a very high level of sophistication in those attacks, the techniques and procedures that they're using. There was a 90% of the time they're gonna be fully undetectable and compared to the vulnerabilities that we're seeing as well and…and the high level of zero day attack that we're now starting…starting to see as well, uh, as well as a consideration on this sort of point of the footprint organisations have now the use of cloud technology, uh, new technologies that they are implementing…um, which makes configuration for…for sysadmins a lot harder because that size of a footprint and it's an ever growing footprint makes that world a little bit harder for them to actually protect, um especially if you're taking on third party vendors and using that infrastructure as a service. Uh, you know the level of your service level agreements with these organisations as well. And they have to be very carefully worded in terms of ownership, roles and responsibilities. Who owns the protection mechanisms and if they allow for third party audit onto…onto that rented container space? Um, if they allow for penetration testing both internal or a perimeter, you know there's a there's a lot of considerations just on that one particular point. Umm, we can look at technological advancements as well.  
We look at the introduction of AI, uh cybersecurity takes a lot of deepfakes at the moment. And we're also seeing uh LLM's like ChatGPT the fact that they coded be stolen by not criminal gangs fell serves to be removed, and these are for spear-phishing campaigns which now makes spear-phishing campaigns a lot harder to identify. And you know, put with that, organisations are allowing your you'll bring your own device, or if I call it, bring your own destruction because you're allowing third party devices onto a part of your network, be it a guest network or not.  
That is to be pivoted against. Sorry, my background is cybersecurity audit and penetration testing, so this is a passion of mine and so I've been solving it for eight years. Um, my background is cybersecurity audit. So yeah, I mean I I'm happy to answer all of these questions.  
When we're talking about those tech…technological advancements, and we're talking about cloud…cloud technology, Internet of things, we then have to take on that cloud technology is now a global network. Um, you don't always know where your data is being stored. When that server particularly is, there's a huge amount of interconnectivity, now globally, that's especially with supply chain dependencies, that sort of international data transfer and those communication networks. So again, that's another factor that's affecting cybersecurity. Umm…put on top of that regulatory constraints as well…uh…these are going to change dependent on where your organisation first is based, but secondly jurisdictions where data is held. So in terms of which regulators you're answering to um…has a huge impact. GDPR, if it is European data. Obviously that has a global impact because it's…it's the European citizens data that is under control by GDPR as opposed to the organisation itself.  
Uh and pulled out of that, there was a cyber skills gap as well, certainly in the UK and there is a cybersecurity skills gap which does then put additional pressure, which then means organisations require to put more investment into actually getting their stuff trained to the to the appropriate level, and the try, try and beat that gap, and also to…to defend against that evolving threat if you will uhm…incorporated within that, I think really we have that awareness and that culture change that needs to take place. And that culture change certainly that's something we do a lot of with organisations is that's obvious that cybersecurity awareness we try to change the culture within an organisation. Umm, so that everyone has that understanding that security isn't just a particular role within an organisation. Actually, everybody has a role to play within that security and that protection mechanism and almost creating that human firewall. I'm not sure that's a term we've heard before, but it's one will go with. And then obviously there…there is that geopolitical element as well. So because we are in the Western world and who our allies are and other geopolitical issues going on globally at the moment that does also have a direct impact. And to…to that question. So yeah, all…all considerations. Really, I'm hoping that can answer your question.

**Interviewer** 15:19  
Umm, OK. Yes, yes, that that's a lot. A lot of information. So basically I think I can hear a lot of because of technology issue. You know the advanced and the development of technology and also some cyber skill gaps between within companies or the…the professionals and awareness and also geopolitical issues, OK.

**UPU1** 15:40  
Yeah. Yeah. So I mean, I mean we when when you when you're looking at this as a as a subject area in my opinion and I'm doing my masters in this as well at the moment.  
So I'm doing a lot of research as well, but in terms of our approach, the approach needs to be holistic.

**Interviewer** 16:00  
Mm-hmm.

**UPU1** 16:03  
It can't be just a targeted approach at technology. It can't just be targeted approach at your…your human risk and your education and your awareness and like culture, it needs to be multifaceted in terms of approach.  
It is holistic. You have to combine and see how they work together and how…how it all meshes. In my particular opinion, that means not just collaboration between private and public sector, but also with academia as well. Because the reality is, is you do need input from all three.

**Interviewer** 16:40  
OK, OK. And then that's go to section C so section C is for cyber defence strategy. So the first question is, what are the overall cybersecurity plans of the UK government and how do you, like in your opinion, how do you evaluate them?

**UPU1** 16:49  
Yep.  
UM, so the NCSC has written a subscription plan for the UK. I think this is my…my comment GSU, but regardless there is a a plan that is set out for for the UK and.  
Off the top of my head. We pretty much spoken about a lot of those things that we've discussed already in terms of protecting critical infrastructure, cyberthreat intelligence, public awareness, uhm, supporting industry. Uh, obviously there is that, that level of international collaboration as well because it's not just us. We do have international partners both in Europe, the US and other areas around the world.  
So in terms of that learning, that sharing of information, IoC (Indicators of Compromise) that we come up against, we need to, you know, we need to have that level of collaboration on a global scale. And again, bringing academia back into it, there needs to be more investment into this kind of research, which is obviously what you're doing at the moment. And so there has to be that kind of investment in research, that innovation to…to new techniques to counter what are new attack methodologies and regulation. So obviously we have the ICO (Information Commissioner's Office), we have the ISO standards, we have NIST, we have cyber essentials, and these are all very, very good, but are now starting to become somewhat outdated with new technologies coming into play. So and by that I do refer to machine learning artificial intelligence, which are now being used and deployed as an attack methodology. So as good as these frameworks are and as good as much as they do try to stay abreast of current. Yeah, working, should we say? I think they need to become a bit more forward looking as well. So think I'll…I'll get off my soapbox now.

**Interviewer** 19:16  
OK. And then the second question is, what are the current cyberthreat precaution strategies and like, yeah.

**UPU1** 19:24  
Uh, yeah. Again, I'll go back to legal and regulatory frameworks to begin with.

**Interviewer** 19:30  
Yeah.

**UPU1** 19:30  
See, we have risk assessments and risk management, which is built into all of these frameworks. Um, so in terms of like precautionary measure, I think that would be good starting point. So doing it, doing what you can with all the firms becoming certified in 27001 as an example, 27035, your BCP (business continuity plan), your instant response, your disaster recovery, those kind of plans that need to be investigated and put into place with again technological means as well as…as the…the policy procedure. Uh, patch management is a…is a…is a huge thing saying you know, on top of these patches because the patches now Microsoft, I think, still has patch Tuesday but they are also throwing out random patches here and there for things that they're finding depending on what infrastructure you're using. And obviously we've discussed subsequently awareness training already several times, in fact, um, but this does become part of your…your sort of preventative measures that you are putting into place. Umm…of technological things that we are putting into place as well, and…and I'm seeing this more and more in industries that as I do talk to industry. So you have two set verification moving away from passwords because quite frankly, passwords are now defunct. So other very large pass phrases will the use of parts of managers. We've seen passwords up to 26 characters now being brute forced, so we all have to now really rethink passwords and rethink actually the…the level of sophistication that we're using and so. All of that, you know, it's…it's all very interlinked. You're secure configuration management. It's all very much interlinked. How we're creating our networks, even you know, we gone on a days of having a flat network where anyone can access anything. You know, we need that Vlans in place. That's that level of segmentation. Umm put into place built on what is threat intelligence.

**Interviewer** 21:42  
Umm.

**UPU1** 21:46  
You know it can't be just a basic template of what a design could or should look like. It needs to be intelligence-led in terms of our protection mechanisms. You know how we protecting our kernel from rootkits. You know, and how we allowing attacker to traverse our networks or you know how we then therefore preventing it. So it's almost taking a purple team approach to having the retina and Blue team working together and saying, well, actually this is how we would do a breach. This is how we would script something and with that in mind, for this level of technology, whichever the technology is by, by and. And you, you're working together to in order to preempt that. Close those gaps. Um, so you know the use of encryption, monitoring, you know, all of this, as I say, as I've said previously, it has to be quite holistic approach. Umm. Even within your service level, agreements with third party vendors again, we need to make sure that there are preventative measures being taken by vendor. So if we are trusting our data in a cloud server, but we need to ensure that there is appropriate segmentation between us and the other clients on a shared server that there is gonna be no ability for traversal by an attacker to…to pivot from one point to another point. So that that's…that level of sort of vendor risk management, if you will. And that will keep us as an organisation, um…compliant with regulators with the law and legislation from different jurisdictions globally, but also keep our data safe, ensuring we actually are not benchmarking yourselves, if you will, against others in our business sector.  
But actually, being leaders in that business sector and I say this to all of my clients, you don't want to benchmark yourself against what someone else is doing because they might be doing it wrong. Quite frankly, we need to always strive to be the leader in your industry and make sure that you have the…the right protection mechanisms in place, the right level of staff training, that overarching holistic view. Hopefully.

**Interviewer** 24:11  
Hopefully.

**UPU1** 24:13  
That will that will take us a step closer to to being, you know, being better prepared, um, more in line with auditors and regulators with the law and actually target hardening each organisation, each business sector. So actually makes the life of the attacker fought harder. So I think yeah, it all goes together. It is holistic and it has to be holistic.

**Interviewer** 24:41  
It has to be a holistic and a complete, more comprehensive.

**UPU1** 24:43  
Yeah.

**Interviewer** 24:45  
OK.

**UPU1** 24:45  
Absolutely, absolutely.

**Interviewer** 24:46  
Yeah. OK. And then so for the third question is it's the following question for the question number 2. So uhm, what…what else can be improved in terms of the cyber threat precaution strategies?

**UPU1** 25:04  
And again, that is a very subjective question because it depends on what element you want to look at being improved. Most certainly a lot is being done in the UK to improve a…awareness culture. Because for me as a hacker, as a social engineer, why am I gonna waste my time attacking a system where I know you're technology is very good when I could just manipulate your people to give me the access.

**Interviewer** 25:32  
Umm.

**UPU1** 25:36  
UM, so I I I'm a great believer in let's address the cyber skills. Let's…let's address the level of knowledge that our staff have, because if we give our staff the tools to protect themselves both at home and at work, well, they're going to protect our company. They they're…they're gonna be our first line of defence. They're gonna actually identify attacks coming in. They're gonna be the first ones to, because if they're getting passed our technology, um, they're gonna Help staff. Our staff will be more prepared. So for me, on the biggest improvements that we…that we are doing in the UK and the statistic that I got from one of my clients earlier this week is that since their staff have been doing the software and training in terms of the attack footprint and people clicking on phishing and spear phishing links as an example, they saw a 66% decline in people clicking malicious links. Uh, and that was in the space of three months.

**Interviewer** 26:39  
Ohh.

**UPU1** 26:40  
And…and now continually gonna be giving me that kind of feedback. They're continually gonna be looking at that…that's that statistics for me, as the years go on because they are wanting to see how the training and awareness piece is having a direct effect on their organisation and a 66% decline. I'll take that all day long because that's a fantastic stat…stat as far as I'm concerned. Uh, so for me that is the biggest improvement that needs to be done to technological improvements are always being done. There's always gonna be budgetary restraints for organisations around that, and prioritization of criticality against except at risk, if you will.  
But that's gonna be very much led by budgetary constraints. Umm staff training, I mean training that we offer is free of charge so they don't have to pay for the staff training. So there are organisations out there like ours that will go out and do free training. So every protect unit, so every cyber protect unit in UK there's 43 different forces in the UK. We all go out and give free protected device and free training to all organisations and residents. Uh, so we are doing our bit to try and lift that level of base knowledge, if you will, alternative for people to pretend themselves. Umm. Yeah, I mean we, we you never you'll never improve budgetary constraints. You know we…we…we do try with C-suites to improve their level of knowledge and their…their comprehensions are say towards cybersecurity. Um, are we winning on that front? I don't know if you have to answer. I test with a mixed bag, but yeah, so they're probably the…the areas of improvement I would be looking at. Obviously I can be used for good and for bad so, but in terms of technology it…it has a very difficult question to answer because every organisation's technology knowledge, you know, hardware, software, etcetera, is all gonna be different. So yeah, but from…from what…overarching answer I think. Hopefully that has answered your question.

**Interviewer** 28:57  
Yeah. Yeah, I can hear a lot of. So for example, you mentioned about budget constraint and again awareness and you mentioned about is 66% of decline of you know to click the phishing link. It's amazing. For me it's a fantastic step as well.

**UPU1** 29:16  
But good. Oh, good, good.

**Interviewer** 29:18  
Yeah.  
Yeah.  
OK.  
So let's move on to question number four and five. Four and five, I think you can answer together…you can answer together because…so four and five is more like because before we talk about and precaution. But now when you are facing the ongoing cyberattack, what are the, what are the strategies and then what do you evaluate them and what else can be improved?

**UPU1** 29:38  
Uh-huh. OK. So, uh, in terms of current cyber defence strategies, if we look at it as a UK centric, so UK PLC if you will. Obviously, we were discussing national cybersecurity strategy, which obviously outlines the overarching uh, cyber defence strategy, if you will. Um, and that is nationwide. We did obviously have the NCSC, so National Cybersecurity Centre and so they are obviously UK's leading authority on cybersecurity, and they provide lots of guidance and advice. They also offer certification to other training organisations, so we as [the name of a police-led cybersecurity awareness programme], are the only UK law enforcement organisation that are NCSC certified. So my team, who are all certified instructors, will we all hold teaching qualifications. We all hold master's degrees. We're all certified and audited annually as NCSC instructors, as are all of our offerings as well. Our offerings are also audited and by an audit firm on behalf of the NCSC to ensure that the messaging that we are giving is in line with that of the NCSC and…and how the…the national messaging should be, and we will be certified on that as well.  
Uh, we've all seen got other frameworks out there and around cyber defence. So sober essentials…um…which is the government backed framework which is basically uh, it's designed around the implementation of basic cybersecurity measures and the effective implementation of those. I know that there are national infrastructure protection plans out there. What they are? I'm not 100% sure um…because it's outside of my remit, but I know they exist. Umm. As you can probably imagine, we do have a lot of public and private partnerships. Certainly, we partner with a lot of organisations firstly to do their training, but we also partner with charities as well to get the messaging out there and to help victims of crime. And we, I can't speak for other forces, but we certainly as a…as a police force, we pay a lot of money in terms of investing for innovation.  
And so we work with a particular university to create new offerings at a huge expense, frankly, that we don't see back. And once we have these new offerings in place, we offering to the public and private sector complete for free.  
So we are investing relatively quite heavily actually. And I know UK government as well is heavily investing in cybersecurity research as well. And…and certainly when it comes to GCHQ, I can only assume there's a huge investment there as well because again outside of my remit, nothing to do with me. In terms of private sector, um, certainly one of the things that I teach is around cyber incident response planning. Umm and obviously this is a…a large thing with all sectors at the moment, because moving away from your traditional instant responses isn't your traditional disaster recovery um…it's now again a holistic approach, incorporating your traditional disaster recovery tactics with the cyber events, which can be quite difficult thing.  
Um, but ensuring that organisations are able to develop a robust plan both to detect and what detector mitigate. But then I'd also say to contain, eradicate and remediate from an attack in order to return to operation. Um, that's…that's a very large piece at the moment. And so I know the NCSC offers their own guidance, which is very similar to mine. Mine because I've developed ours, is based on my audit experiences based on not only UK centric frameworks but also global frameworks such as NIST et cetera. Umm. In order to…to again build a almost gold standard, uh, I don't back it out. We then designed again with academia and instant response tabletop, which is very different to anything that's seen on market in the private sector and in my opinion, it is pretty my opinion is the closest to a real world event that you run to.  
So there's only key elements. I think that will play to UK PLC inverted commas.  
They're cyber defence strategies that we have in place. There's always going to be emerging threat. Um…that you can do best plans for, but again they all know none knowns. So as much as we will expect them, you're not always sure of what you're gonna be facing. So you have to try to make it fit. In terms of what could be done to improve these things. I think in terms of legislation, certainly the Computer Misuse Act has been amended a few times, but in terms of the relative speed of evolution, um, in this arena, that document is very much outdated.

**Interviewer** 35:59  
OK.

**UPU1** 36:00  
Quite possibly not fit for purpose, so I know he's had…it has had a number of amendments done to it over…over the years, but I don't know they're…they are looking currently. I believe at more amendments to…to go into that document. But certainly yeah, it…it in my opinion and it is my opinion, not that other police, it does need amending because I don't think it particularly, with…with current threats that are taking place around the world on that sort of global theatre, I don't particularly mazed if it is fit for purpose at the moment because there are new technologies that are just hasn't considered. So yeah. So, definitely. Hopefully that answered your question.

**Interviewer** 36:41  
Mm-hmm. OK. Yeah. It's so that we have to keep up with the pace of the ever changing of the, you know, the hackers and the cyber attackers. They…they like, obviously they have the more advanced skills and technologies and we need to keep up with the pace with them. So we can tackle them.

**UPU1** 37:03  
Yeah. And sometimes I think we actually need to try and get ahead of them.

**Interviewer** 37:09  
Yeah.

**UPU1** 37:10  
Because you know, work working with private sector vendors such as Microsoft or Apple, you know the…the…the larger people, uh certainly that most organisations are using their technology. You know, if we're looking at server stacks, we're gonna go back to Unix systems, which is, you know, my preferred platform anyway. But for your day to day running of organisations that are using, you know, MacOS, or they're using a version of Microsoft. I know that there's a lot going on in those spaces.  
Umm to well obviously protect the brand and reputation, but also to protect their client base and their infrastructure. Uh, but I do…I do feel sometimes that they're probably firefighting more than being innovative. So yeah, if we can get organisations that to actually start preempting the text, uh, which I know they do…do a lot of work for, you know, I'm, I'm not trying to take away from the good work that they do because they did a fair amount of research and innovation themselves. But I think they needs to be more focused around that so we can actually…in terms of a in…as an investigator, I'm always a step or two behind.  
And an attacker, although in recent years in the last four years, that's changed.  
So we have devised something in local focal police CyberAlarm. I'm not sure if you've heard of that before. Um, but if you go to police CyberAlarm website, it has a full explanation as to what it is. But what that system does allow for for us as investigators is it allows us to see attacks as they are happening to organisations you're signed up. And we can literally parallel that attack. So instead of being a step behind, we can see it happening in live time. We can identify perpetrators easily. We can identify infrastructure easier and…and therefore we can take down that infrastructure…infrastructure a lot faster. We…we can bring them to justice a lot faster. Um, so there are initiatives like that. And again, this is an initiative that is offered to the public and organisations completely free of charge, but has had huge amount of financing from law enforcement go into it so that we can do our part for UK PLC to…to try and combat that type of crime.

**Interviewer** 39:29  
OK, OK. And then I think that's linked to question number six and seven because now we are going to talk about the reflection measures. Obviously it's after, you know, you've been experiencing the cyber attacks. So what are the post cyberattacks reflection measures and how do you evaluate them and what can be improved?

**UPU1** 39:55  
Yeah. So. So in terms of post attack, this is gonna be, you know, our…our learning phase, if you will. You know, we're gonna…we're going to do analysis around how we responded to that particular incident. We're gonna be doing root cause analysis because we need to understand points of ingress points of egress, um, how vulnerabilities have been exploited, why we had that weakness. Uh, um, you know, within that incident response so analytics, if you will. Uh, there's a lot of evaluation there. We need to conduct an impact assessment during that evaluation. So not only how it has impacted us, how has it impacted our staff reputation, the systems that we're utilizing, the data that we hold as an example. Uhm, but also it could have a direct impact on supply chain. Uh, so we…we…we need to do actually quite in depth impact assessment there. Uhm, obviously we do the calls all of a…of an incident. We're gonna be documenting throughout because we need to have that audit trial.  
We need to have be able to rationalize decisions made, tactical options that were available to us within that sort of snapshot of time. I always advise organisations that yes, we do need to document or rationalisation of decisions that we've made. But actually what we do also need to document is the options that we had available and the decisions we chose not to make. And we need to rationalize those as well because the reality is if there is a tribunal or any type of civil litigation down the line, people are going to question well, I believe you had other options available to you.  
I believe you should have done this. The truth that matter is they weren't there at the time, and if you haven't written it down, people gonna…are gonna think that you haven't considered it. It's not been a consideration actually do document that it was a consideration and there are reasons as to why you haven't chosen those tactical options. It could be a financial gap. It could be a skills gap. It could be a resourcing gap. Be human resourcing or technological resourcing. There's a huge number of vectors as to why you won't take a particular tactical option, so all of this needs to be documented and needs to be reported accurately. Uh. When we're doing that root cause analysis, we're doing that digital forensics work. You know, we need proper chain of custody. We need to make sure that people are working to the same level of competence.  
Uh, so there's a lot there to actually be considered in that almost learning phase. Um…you know when we're looking…past there because we do need to remediate, but also within that remediation, we also need to put and mitigation for future attacks. So we need, you know, there's a lot that needs to be considered. There's a lot of things be communicated, not just internally but to third party suppliers and your supply chain on a greater picture, not your…your third party suppliers to you, but possibly if you are within a supply chain going to other vendors. You know, IoC (Indicators of Compromise) needs to be communicated because if you can assist them in target hardening themselves as well as target hardening yourself…want to build trust but also makes your…your business sector a lot harder to attack and to hopefully make it a lot and a lot more difficult for attackers. And within that, within that supply chain, I think we also need to conduct a…a third party assessment, if you will. So if we are allowing third parties access potentially to parts of our network, be that through VPN or not, um…we'll actually do they comply with the same security standards that we hold internally because are we then allowing another vendor who has lesser security controls access to our infrastructure potentially being that weak link in that chain, if you if you will. So it almost needs a systematic review. And on that reflection of what's just occurred, the 5W's, you know, Who, What, Where, When and Why, in order to identify, remediate and improve. Um…is it's…is all good and well…being in line with compliance in frameworks? But if that framework actually isn't offering you enough security, I think we need to go above that and that's where we gonna get the learning for…for this. Because we do see organisations all the time who are NIST compliant, who are ISO 27001 compliant, they're certified, but they're still being breached. Well, that to me begs the question then is as good as these frameworks are? And they are all very good frameworks. Are they…are they sufficient? And the only way you wanna get that is from this kind of learning, so yes.

**Interviewer** 45:38  
OK, so I see. I think um…then, because you've been mentioned a lot of, you know, the awareness and training. And so I think that question number eight and nine and it's about that. So I want to ask you, I believe you've mentioned before, so how do you evaluate the general awareness of cybersecurity and you know the government plans, governmental plans to enhance their awareness?

**UPU1** 46:17  
Yeah. So. So for…for question 8, then um so general awareness of security amongst the general public. I'm I I generally think it's quite poor if I'm honest. Uh. There's…there's a huge lack of knowledge in the public space. In fact, no, that's that's wrong. That's incorrect. There is a lot of knowledge in the public space that's available. I think in terms of awareness to the possible threats that are out there, there's a very poor level of awareness within the general public, certainly a lot of the organisations that I go to for the first time. And we train them on baseline levels of knowledge around cybersecurity. People are unaware of very basic attack methodologies. They're very unaware of social engineering tactics and techniques. Um, so as a there I say. As a generalization, I'm gonna say that level of awareness out there is very poor within the general public. In terms of current governmental plans for education, for the general public, I actually think the very, very good. And obviously I work for a government body. We do as much as humanly possible to go out and train as many people as possible over the last of the last four years. We and I can only talk for stats for my own particular unit. We've trained 53,000 people. Uh, and we are continually trying and striving to train more because we want that message to go to get out there so that we can raise that level of awareness. We can raise that level of knowledge that is out there and protect people for better. Umm.  
From what is naivety people is aren't aware of it, because if they don't work within this particular sector, umm, they don't have any real need to have that knowledge.  
Or at least that's their perception. And so yes, certainly from a government level, there's a lot being done. There are a lot of initiatives out there to train the general public, to train private sector organisations. In order to make UK peel see a much safer place for everybody to…to live and work in. And. So yes, I think that answers that question, I hope.

**Interviewer** 49:03  
Yeah, I think that's amazing. What you've done, you know, to train people for the general public and so and that's go to question number 10 and the question number 10 it's about the future cybersecurity talents. Do you know about the governmental plans to cultivate the future cybersecurity talents? Maybe in schools or outside of school? And how do you evaluate them?

**UPU1** 49:29  
Yep. So there's a lot that goes on in that space. I know the NCSC has a cyber schools program, I think it's called and, which looks to identify and basically nurture young talent within the schools and get them working on the right side of the law, so to speak. UM, it provides, I think from memory and you have to, you have to.  
Excuse me, this is this is from memory. I believe they provide educational resources to schools. They also have, I think, CTF type competitions that they get the kids involved in and…and I think that children from the ages of 11 to 18, from memory.  
Um, there's a number of initiatives, so CyberFirst, this is certainly one that law enforcement get involved in as well. Cyber Discovery, I believe, is another one.  
Uh, and and I'm not sure if it's in every school in the UK, but I think there are cyber hubs for schools. But I'm not 100% how they…I'm not 100% sure how those work. And but it's all about engaging students again, raising that level of knowledge if they do have a particular aptitude for that skill set, the nurturing that skill set but for the right reasons and. CyberFirst, I think CyberFirst actually goes up to undergrad level, I believe. and I'm not 100% sure on that, but I I I've got a feeling it does. So it's 11 to 21 uh, but I believe within CyberFirst as well, it opens up a, a, a, a career pathway…um… for people who have that interest. And it’s….what did I call that? Uh.  
STEM, but if it is, uh, science, technology, engineering and mathematics, I think is another program that is out there. Uh again to…to cultivate that's…that sort of level of knowledge within people and…and…and that's again open to all background regardless of whatever your background is that's open to you. And I think now there's apprenticeships in cyber as well. I think some organisations are doing an apprenticeship scheme, and again, we don't do that so I’m not quite sure how that works. But, from I heard I was speaking about apprenticeships and there's obviously your traditional academic routes and so you know, your…your undergrad, you're postgrad PhD levels of…obviously that your degree programs also your research programs that are there within academia. Um. CPD (Continuing professional development) because I…I have to do CPD every year. So yeah, obviously CPD is there, we can workplace and. Yeah. I mean, I think, you know, I'm…I'm…I'm moving slightly away from your…your question if I'm honest because it was very much around schools, wasn't it? And yeah, but there…there certainly is a lot that happens in the UK from government all level down. So yeah, certainly I think we're moving in the right direction.

**Interviewer** 53:11   
Yeah. That that's actually a lot of…umm, the programs you mentioned as like…like for example Cyber first because I yeah, I went to their websites before and to google that so I know they offer a lot of opportunities like apprenticeships and then maybe the you have some program, school things like that.

**UPU1** 53:20  
Mm-hmm.  
Yeah.

**Interviewer** 53:38  
So that's go to section D. So section D is for the public private partnerships in terms of cybersecurity. So the first question is, what do you think about the idea of public private partnerships? And do you think it's really helpful to…in terms of to enhance the overall cybersecurity?

**UPU1** 54:03  
Yeah, I mean, I mean this is something certainly is already happening in the UK, certainly something that we do and I know other…other police forces do it as well and certainly government and governmental level. You know, I've…I've…I've sat in the Commons (House of Commons) when I worked in in audit, um…working with public and private sector. Uh. For us, there's certainly is a cyber special scheme, so if you have a cyber specialism and you want to become a special constable but you don't want to walk the streets and deal with violent crime, whatever it is. We do have a cyber specials program where they come in and use their specialist knowledge to assist uh with cyber configurations, preventative measures, et cetera building….and tool sets if…if required and so on. That's certainly is an initiative. And there's a lot of networking that goes on between private and…and public sector. Certainly we and other forces go to the international cyber expose and I go to Black Cat every year.  
There's loads of networking that goes on and collaboration work and collaboration pieces between public and private. Umm, we go to some of the season groups, certainly London…um….and there is information sharing and collaboration there for what they're seeing. Obviously is all done other Chatham House rules. And I've just been invited to…to join a…a Worshipful company. I won't name them because that would be a little bit unfair of me, but it's within this environment. Um, which I'm considering joining, so there…there was a lot happening in this space in terms of partnership work and at all levels. I'd like to say so. It's not just that that sort of a local level, it's at a regional, national level. I think that's…that's…that something is in place in the UK already. So so yeah.

**Interviewer** 56:13  
Ah. Yeah. So no, sorry, sorry to interrupt.

**UPU1** 56:19  
No.

**Interviewer** 56:20  
Uh, OK. So, uh, then let's go to question number two. But you just told me about a lot of the how they work together. So can you tell me more about that? Because you mentioned because I want to know the mechanisms like for some you say you said information sharing and also like how do they cooperate in terms of information sharing or in other aspects.

**UPU1** 56:35  
Yep. Umm. So the biggest information sharing platform that we've got moment is Police CyberAlarm. So that is how organising it, organisations are giving back as well, because we use we have analysts who look at that 24/7 and…and they collate that information into trend analysis at every single level. So local, regional, national and then global levels, must we look at global attacks attacking UK PLC. And anyone who is signed up to Police CyberAlarm gets all of those statistics. So it doesn't just give you information about your one organisation or your one particular area that you're in. It gives you everything inclusive of the top 25 IP addresses globally attacking UK PLC, uh…top 25 appear addresses within the UK, attacking UK the obviously umm.

**Interviewer** 57:29  
Mm-hmm.

**UPU1** 57:34  
It even breaks it down by business sector. So there is that kind of information sharing. There's obviously sisp (Strategic Information Systems Plan), so people who start up to the sisp from a governmental level down is huge information share in there. Certainly in some of the offerings that I do, certainly the instant response because it's done under Chatham House rules, organisations there, explain to me IoCs that they're seeing or attack methodologies that they're seeing other against them or others in their sector that they're aware of. So that is shared with us.   
I also share new trends that I'm seeing with my clients and I know I'm not the only one that I know is loads of offices that do that. Uh…um…when we go to um, I called.  
So Community event, roadshow type events and we obviously speaking with people there because we want to offer the free training, but we do obviously get the questions about trend analysis, what we're seeing, uh, how…um…what the likelihood is of bringing offenders to justice and like how investigations actually happen, we obviously we've can't disclose too much about how investigations happens because there's a lot of sensitive information and tactics. But there…there is a lot of and sharing in that sort of extent. Umm, there's lots of cybersecurity forums as well where we go and talk about methodologies that we're seeing. Um, and again, it's all about target hardening that that that's the…the main sort of reason for that kind of level of information sharing because we want people to target harden against what we are seeing. So, yeah, obviously NCSC engagement as well the NCSC, on their website, offer a huge amount of information. The Action Fraud website offers huge amount of information trend analysis for organisations as well. So it's very public information sharing, but you know we…we certainly sign post all of these places to people. And so yeah, they're not very sophisticated mechanism sometimes, but sometimes are the best ones. So but yeah.

**Interviewer** 1:00:03   
OK, so I want to ask more about this public, private partnerships. Uh, so how can you contribute to this? Partnerships. Uh, as a public sectors and also how can the private sectors contribute to this partnerships, in the opinion?

**UPU1** 1:00:24  
So. I've already discussed Police CyberAlarm. Umm. In terms of private sector contributing back because that they're allowing us to see that, that level of data flow, uh, you know, identification of abnormal courts being used for attacks etcetera. So…so from…from them to us, that's a very, very good way of, of or partnering…um.  
Certainly with expertise that they may have as well. We have had private firms offer their expertise if we've needed it, and also vice versa, um. For us...um…When it comes to organisations on boarding, they've actually made some of our training material mandatory to all staff on…on boarding and they also have made it mandatory for…umm, annual CPD as well. Some of our….some of our…um…offerings as well before, sorry….um…are actually CPD certified as well. So uh, I'll based on briefing as an example, Office 2 CPD points. So for anyone who comes to our briefings, they will get a CPD point, certainly if they hold and qualifications that require CPD. And a lot of organisations utilize that mechanism as well for their staff to prove that they've done the training, but also for their cyber insurance as well to prove that they are investing in staff training. Uhm. So I'm not quite sure I answer your questions for the moment, honest. Yeah, I mean, so certainly with the charities and we do a lot of work together and and…and certainly they put us into different groups of people from all sorts of backgrounds and in terms of getting them trained up in, in, in cybersecurity in that that level of knowledge. And so yeah it's again quite holistic approach to…to how we do it. Um…and obviously a lot of what's all about now is at local level. Uh from national level and yeah I mean from national we you could CRC (cyclic redundancy check) is what…CRC is regional but they do answer to…to a national board and they offer very similar training to us. And they also offer additional offerings as well. They also work with the CRC. CRC's work is actually very well with academia as well, because they allow students to actually get paid a day rate to go and assist on penetration tests on cybersecurity audits, stuff. So it's also building the skill set for the students to go into the wider world. But actually what it does as well, as a byproduct of that, is we're almost infiltrating, if I can use that word, private sector organisations with, you know, graduates who have a good working knowledge of what is available from governmental level down to local level in order to assist private sector organisations in preventative measures to not become the victims of crime. Does that make sense?

**Interviewer** 1:04:02  
Yeah, yeah, totally.

**UPU1** 1:04:03  
Yeah. Cool. I'm good, good guys.

**Interviewer** 1:04:06  
Yeah. And then how about the difficulties?  
Like, have you ever encountered any difficulties in terms of the partnerships so far?

**UPU1** 1:04:15  
Umm, I'd say we have. Yes, certainly in the environment that I work and obviously work within the financial heart of the of the country. And so the organisations that we have here literally spend hundreds of millions every year on preventative measures, mitigating threat, you know. It…it was when we were very uh first established quite difficult to get into these companies to offer our trainings and…and and our services to them because they are free and people sometimes look down their nose at free training and saying, well, we pay all of this money. We're paying all of these third party vendors. Um, what are you going to bring to the table, really? Um… But actually, once we did break those barriers, um, we…we're only a team with seven people in my office. We don't have any budget for marketing. We don't do any marketing. We or we obviously get to this cybersecurity forms and what have you, but all of our work comes through word of mouth. So we get recommended to people through supply chain etcetera and to…to the point now that we have people coming not just nationally to us for our training, but internationally as well. Um…so we've been to a number of countries now, I'm off in 2 weeks somewhere else in the world to train out there. And we're not just training private industry, we're also training other law enforcement bodies around the world. Uh, so when we were being first established, yet the difficulties were…were many, if I'm honest. But I think that's the same with any new organisation when you're trying to break into a market, you're gonna face those, those those difficulties in actually getting on to that market and breaking it. And we still occasionally get organisations who try to question the validity of our experience and our knowledge. But then you know, we can say to them we'll look at us on LinkedIn, they see these are all credentials.  
These are the trainings that we have. You know we've got ISO 27,001 league, all implementers, we've got penetration testers. My background is obviously auditing and penetration testing and we have offices with system and seasoned qualifications. Other malware reverse engineer. So we have a multitude of what are nationally accredited and privately accepted qualifications. So those boundaries now are broken quite quickly because we can turn around so well. Actually what I do have all of these qualifications and we do have a vast knowledge base. We do have direct access to national databases to the actual database, Global Cyber Alliance databases.  
We have access to a huge amount of information and everything that we do is intelligence-led. So yeah, we don't particularly have those difficulties anymore.  
If anything, we've got probably more work than we can handle because the words of mouth is spreading quite quickly and people are very impressed with the amount of offerings that we have and the amount of information that we do share. And obviously free of charge. Um, so yeah, I think the difficulty now is that we probably don't have enough staff.

**Interviewer** 1:08:10  
OK, I see. And so that will be the last question right now because you, yeah, you've talked about a lot of your experiences. So I'm not going to ask you that question again. So for the future partnerships and what in what, as in what direction do you think that will be to improve or to make this partnerships better in the future?

**UPU1** 1:08:29  
Umm. I think future partnerships are gonna be very much international. I think as a…as a country where we're becoming better and better at what we do and certainly about messaging culture change, the technologies that we're employing and the fact that we are having that communication between private and public sector, I think we are very much on the right path as a country. I think from an international level, umm, we have very, very good connections on an international basis. And we all quite cohesive, but there's always room for improvement. And because I don't think I will ever be…be perfect, and certainly the effect that Brexit has had with Europe, we, you know, without go overseas production orders that have just come into play as well. They're…they're currently being tested within the UK, they're not live at the moment. They've been tested by the NCA. um, there…there's a lot of work being done on those improvements, so only on that international picture. Umm, but I don't think we're there yet. I think there's a lot of work to go. So. So yeah, I think that hopefully answers your question.

**Interviewer** 1:10:07  
Yes, yes, definitely. And so sorry. So I want to ask more about what you just said before because like you, you mentioned a lot of the experiences, but I…I still want to.  
Ask more about can you give me like more examples of your experiences on this partnerships? I know you’ve mentioned some of them before, but.

**UPU1** 1:10:33  
Yeah. Yeah, I mean it, it's very. It's very difficult to answer that question without giving information away into, in regards to business sectors that I work with clients et cetera, which is obviously not willing to do because I don't have their permission to do that.

**Interviewer** 1:10:47  
Mm-hmm.

**UPU1** 1:10:51  
And certainly in regards to and, the trading is very, there's very little that I am giving you lots of to those to those partnerships and obviously in regards to those partnerships because they are well established now and we do…do the vast majority of the cyber training for a lot of organisations that are on…on our books and.  
That that it's just very smooth running, if I'm honest. Um, are we taking work away from other private sector training companies? I don't think that we are because the…the…the area is so vast and we don't offer everything and our other organisations that offer different methodologies of training to what we do, we certainly don't do any e-learning or anything like that. And I personally very much don't believe in e-learning because, in my experience, and certainly from what I'm told from my client base is that people just skip to the end, answer a couple of questions, or just click a button to say that they've done the training. But the reality is, is they haven't done the training because they don't want to sit there for half hour, 45 minutes of their life with an e-learning package because it's boring. Umm. And I don't see the benefit of it. And there are ways to cheat that system. Uh, so we're…our training is all either in person virtual or a hybrid of the two, regardless of where the organisations set globally. Yeah. So, so we do work with partners in terms of methodologies of teaching, so to speak and…and how to get the best out of that.

**Interviewer** 1:12:51  
OK.

**UPU1** 1:12:51  
So yeah.

**Interviewer** 1:12:51  
So those partners, they are from cybersecurity firms or some training companies?

**UPU1** 1:12:59  
No, no. So these…these partners will be from all over many different business sectors.  
We don't, we don't partner with. So anyone who makes a commercial package or a commercial training, we will not partner with because we are a free service.

**Interviewer** 1:13:20  
OK.

**UPU1** 1:13:21  
And we will not allow them to make a profit off of what is a free service open to absolutely anybody, because morally and ethically, that's a very, very wrong. Uh, we have had vendors, Tracy that in the past and tried to hide that. But they're very, very quickly caught out. Umm, we always said that we will not go to any talks where people have to pay to be there. So any forums, if people have to pay for the privilege of being there, we will not talk at those because again we have that ethical and moral question really of well we will give it to you for free. We're not going to give it to you a paid event because that's not, it's not. So they're the sort of…markers if you will, that we put down with organisations. If people are doing a free event for their staff internally or even for people if it's a multi…multi occupancy building with multiple organisations within there. If they want to invite those other organisations to train that we're giving on the basis that they're not charging those businesses, we will happily do that and that that is how we partner. So we don't partner with organisations in the traditional sense. Um, but we will partner with them in terms of they will mark it us, uh, through word of mouth, if they are happy with services. Uh.  
They partner with us in some instances that is very, very rare that this happens, I have to say, very rare. They will put our logo with that they work with us. Uh, because we our reputation is at that point now that it is in good standing. Uh, but in terms of partnerships, when there's any commercial benefit to anybody, that doesn't actually happen. Uh, which is what…The only people we've really partner with in a traditional sense are charities because they're not for profit. We're not for profit.

**Interviewer** 1:15:35  
OK.

**UPU1** 1:15:35  
Uh, so that in in, in the traditional partnership sense, that's the only partnership we will do. Uh, we do partner with organisations who will have their own client base that are generally SME type clients who don't have the financial capability of paying for training packages and those organisations will partner with us because they will then put us into these SMEs so that they can better protect themselves. But those SMEs will form part of their supply chain in some respect, so it is beneficial for them in that respect, because their supply chain of getting some level of training for free.

**Interviewer** 1:16:26  
OK.

**UPU1** 1:16:26  
So yeah, hopefully that answers your question.

**Interviewer** 1:16:29  
Yes, definitely a lot of information and thank you so much. So I think that's it. So let me just press stop.

**UPU1** 1:16:40  
Wonderful.  
Do I do I get to see your final work?

**Interviewer** 1:16:46  
Yes, sure.