**Interviewer** 0:05  
OK, now we are recording now. So let's start from Section A and Section A. It's for basic information and for the first question I will put you in public sector because you are from the the yeah, the police….force. Sorry. And then so the question number 2 can you tell me about the you need you work for?

**UPU5** 0:35  
Sure I am currently I work for the [the name of a regional organised crime unit]. I specifically work in the cyber unit there and I run the cryptocurrency team.

**Interviewer** 0:41  
Uh huh. Mm hmm, OK and the question number 3 and how long have we been working for the unit?

**UPU5** 0:59  
This particular unit I've been here for just over a year and a half now. However, prior to that I was within [the name of a regional police cybercrime unit] as an investigator for five years, so I suppose four or five years maybe. I remember time takes on. So yeah, I've been in cyber in some way, shape or form for the past five to six years.

**Interviewer** 1:17  
Mm hmm. OK. And then number 4. And So what? What position do you hold in the unit you are working for or before? Yeah.

**UPU5** 1:34  
Currently I'm a I'm a Detective Sergeant. But prior to that, I was Detective Constable.

**Interviewer** 1:41  
Mm hmm. OK. And then the question number 5 is, what are your main responsibilities right now either now and also the previous job when you are working at the [the name of a regional police cybercrime unit].

**UPU5** 1:57  
So fixing on the the previous one as a DC (Detective Constable) my role was to investigate cyber the crime that came into us. So, we would receive a report, be it by [the name of a regional police cybercrime unit], the 999 system, or report in by action fraud. That report will be given to us and then we would engage with either the individual or the company and determine what had happened. We would investigate that impartially to a point where it would either be possible to take it to CPS (Crown Prosecution Service), find some other means of resolution for it, or the case might take no further action.  
So at that point, if it was a case to build, I will build that up and take it through the the Court system. Ultimately, to the point of prosecution charge. The the all the bits that go along with that so investigation or building advice support for the units. We did to them on scene at digital forensics. Dealt heavily with cryptocurrency when I was there as well.

**Interviewer** 3:11  
Mm hmm.

**UPU5** 3:11  
Investigation and seizures, things like that. So currently you know, I managed the cryptocurrency team specifically. The unit itself deals primarily with investigation of cryptocurrency and it's used within criminality be that whatever criminality it is. However, it's a cyber heavily focused on cyber crime as that is the unit that I sit with. But as a support unit we can provide support out to any kind of criminality that's out there. So drugs, stock, web fraud, whatever's going, we will support that unit. But I managed the investigators. I provide training, I provide inputs and things like that to others within the the forces that we manage.

**Interviewer** 4:02  
Mm hmm. OK. Uh, so when you said you provide training is providing training to the policemen, police or the you know, the general public?

**UPU5** 4:15  
I'm not doing it sort of, not the general public, but some kind of public sector infrastructure. So we might provide an input around cryptocurrency to prison service. Or in this case, we've done it to magistrates courts so they can understand better the requirements of any court orders that we take over to them. In the training aspects for sort of internal, I will train officers around it the investigation, identification and things like that. So I train, the investigators that I have within my unit to at very, very high level, whereas it might be the investigators and police officers that are on scene that are arresting people. I will also train those people as well.

**Interviewer** 5:00  
OK.  
Then let's go to Section B and Section B. It's for the some more comprehensive question about cybersecurity. So the first question is. In your opinion, what are the major cyber attacks in the UK and what are the modus operandi and you can also give some examples.

**UPU5** 5:26  
I am the majority or the major, major cyberattacks in the UK are all gonna be ransomware. So the various different ransomware groups that affect companies and target the large scale companies at the moment they are going to be the primary impact factor nationally at the moment as being a drain on funding and resources because they they cause humongous amounts of damage. That is the the large scale aspect of that. And the modus operandi for that is you, you end up with a ransomware group. And you generally have someone who provides said ransomware and you have what's called an affiliate and the affiliate will use the ransomware. So it's almost like you buy a subscription with your ransomware and the person using it will find a way onto someone's network, deploy that ransomware, and then target them for the extraction of data, bringing them back in to make that extortion, blackmail request for money later. And the system will help progress that.

**Interviewer** 6:32  
Mm.

**UPU5** 6:32  
I suppose that's a large scale sector of that. I mean examples of of those kinds of attacks. They are. They're all over the news at the moment. Things like Conti ransomware, things like blockbuster, things like I'm trying to think now. So many of them that are out there in different strains. We have is an old one. Many others have taken large scale targets and just caused mass amounts of problems.

**Interviewer** 7:04  
Mm hmm.

**UPU5** 7:05  
I suppose the other aspect is you've then got the…the ones that affect the public most cyber attacks and they are not necessarily cyber attacks. They are more phishing attacks where they attack their particularly SIM swapping and things like that to get access to their phone details. They want access to their bank details, so hacking their accounts. Getting them to give over passwords, or the 2FA (Two-factor authentication) codes so that they can get into those accounts and then use them for further criminality. IE swapping out their their phone number on their bank account so that person can then get access to that. Rearranging post and making payments on Amazon, taking their…their social media status online to use that for various other purposes, be it online marketing or nefarious issues like fraud scams. So that is primary aspect there. Although it is cyber. It's not necessarily hacking. It's more.  
What we call it? I want to call it fraudsters, but it's social engineering. That's the term I was looking for. Phishing, smishing, social engineering. That's probably the one that affects the public most.

**Interviewer** 8:18  
Mm hmm. OK. And when you talk about the ransomware and so the the, the criminals, they, they are more inclined to ask you to pay the ransom in cryptocurrency or any other kind of ways.

**UPU5** 8:43  
And to where it's primarily now cryptocurrency. I haven't heard of a ransomware requesting a deposit in, let's say, fiat standard currency for a very long time now.

**Interviewer** 8:55  
Mm hmm. OK, so normally and the first question that the the major one could be ransomware and some phishing attacks maybe and then umm, social engineering it's the three types you mentioned, can I can I conclude like that?

**UPU5** 9:18  
Yes you can. I'm quite happy to conclude like that.

**Interviewer** 9:22  
OK, then let's go to question number 2. So what are the major targets of cyber attacks in the UK and what are the reasons behind?

**UPU5** 9:36  
Ultimately, if we focus on ransomware, it's large companies that can pay a large ransom. It is entirely monetary motivated and you've got the the single and triple… single trouble and triple extortion. We will encrypt your systems, you pay to have your systems decrypted. We also have extracted all of your data if you want that data back and not on the Internet. We will charge you a ransom for that. So it is entirely.  
Financially driven for pretty much all of the hacking us, all of the hacking aspects out there have a financial motivating aspect to them.

**Interviewer** 10:23  
OK. So military motivated, there are some of them, they are military motivated and most of them they are financially driven.

**UPU5** 10:35  
They they're pretty much all financially driven.

**Interviewer** 10:37  
OK, OK. Yeah. Did you want to say something wrong or not?

**UPU5** 10:44  
Not, not really. Not, no, no, I'm fine.

**Interviewer** 10:45  
OK. Then that's move to question number 3. So what are the factors affecting the cybersecurity in the UK?

**UPU5** 11:02  
Let's try to think now. In short, I don't know if the…

**Interviewer** 11:12  
For example, in like awareness or some political reasons or some like like you said, the financial reason and.

**UPU5** 11:24  
So the affecting companies is probably again, finances. So cybersecurity aspects around that is usually the last thing that a lot of companies think about. They're usually thinking about sales, think about how to do this, how to do that, the security off the back of it is not usually the best when they're looking at that. They're also putting down or not doing the relevant updates or using obsolete software or using obsolete hardware which allows for vulnerabilities to get in. So that is probably the primary aspect that affects companies and how they're affected. The secondary aspect is going to be that social engineering aspect and it is going to be knowledge and understanding on part of the victims or those who are affected by phishing. So the targets, a company employee who's going to give out their password or pin number or compromise their own e-mail account within there when they hit that, that phishing e-mail, they're going to click the link because they don't have the knowledge or understanding to tell them not to.

**Interviewer** 12:31  
OK. So it's more like the cybersecurity awareness, the knowledge they are.  
They don't have enough that kind of knowledge.

**UPU5** 12:41  
General. Companies. It can be. So it it's too strong. So when it comes to a company, as in an attack where you have a technical attack upon a network or system that revolves around exploiting a vulnerability on a network or an…a vulnerability in software that usually is impacted by old systems, lack of updates, lack of security awareness on the part of those upkeeping it, or lack of funding into the cybersecurity aspect of their business to upkeep that. When it comes to the workforce and the social engineering driven side as in passwords to FA pins, things like that, then that's the knowledge side that is there...the driving factor. It depends on which aspect you're looking at really.

**Interviewer** 13:33  
OK.  
OK, let's move on to section C and Section C and the question are more related to the cyber defence strategy. So for the first question and the second question, I think you can answer together because so I'm sorry, no it's it's, it's the next one. So for the first question is what are the overall cybersecurity plan and of the UK Government that you know? And how do you think about them. How do you evaluate them?

**UPU5** 14:11  
OK, so the UK forces use what's called the four P plan, so they use a process called prepare protect, prevent and pursue. Now prepare is obviously impact everything prior to an attack, so hardening that that target, making people aware, running all those aspects around to make sure that companies don't become that…that victim to start with.

Then have we move into protect. Protect is very much a case of I have been a victim of cyber crime. How do I not become a victim of cyber crime again? It might be awareness campaigns. It's going to be dealing and talking to victims of places like the Cyber Resilience Centre, getting involved with companies to making sure they're…they're hardening the target after the attack. So how do you protect your company and your…your people after that? So you have a various different groups out there that involve and engage themselves out in the company. So if you look at the, let's say, our pages [the name of a regional organised crime unit] for example, we have a cyber protect team. They will do aspects of cyber prepare as well in that. If you own a company small to medium sized company, you can request an input from them for your team or for your management around cybersecurity to…to help you protect your stuff. You have the…the aspects a lot around this of awareness programmes, a lot of marketing, a lot of advertising and a lot of information being put out to people.  
Prevent is a little bit different. To prevent involve getting engaged with those who are….Let's call them in risk categories. So like young people who are exposed to IT, you have those who are using security systems and might not have that awareness that they are committing offences. It's about engaging with them to pull them away from criminality and show them how…how the skills should be properly used or engaging with them to see and find out what we can to try and pull them away from that criminality aspect. The other side of prevent is once an offence has been committed and a person has been identified, prevent will engage with that person. Try and help them come out of that spar and get out of that criminality and prevent is more about moving people away from crime and cyber criminality than anything else.  
The pursue aspect is exactly where I sit, it is the investigations. It is tracing those suspects and offenders and bringing them to justice so that those are the strands that we have. It's always those four Ps, prepare, prevent, protect and pursue.

They also work across other…other law enforcement areas as well, not just cyber, but as a national strategy. That's the one we're working to correct.

**Interviewer** 17:24  
OK, so the four Ps I think the…as you explain like the prepare, protect and prevent, they are more like the precaution strategies and the pursue. Like you need to deal with that right now. Is that correct like?

**UPU5** 17:44  
Umm yeah. If we go with. Prepare, protect and pursue. They all fit into that pretend preventative measure aspect. Whereas persue is very much a reactionary aspect or a proactive investigation where you might have identified somebody who might be targeting something. So it's investigations into criminality rather than everything else which sits on the outside there.

**Interviewer** 17:50.  
OK. And let's go to question number 2?

**UPU5** 18:14  
Mm.

**Interviewer** 18:15  
Yeah. Then question number 2 is, what are the current cyber threat precaution strategies? Like you said, the prevention strategies that you know and how do you evaluate, evaluate them and I think number three we you can also answer together. So and then how can what else can be improved in terms of these strategies?

**UPU5** 18:39  
Don't really think I can answer these ones effectively for you. I might be the wrong person to do that. Reality is that I have been in pursue now for X amount of years and I haven't stepped outside of that to do the protect prevent side, so creating those precautionary measures is not really something that I'm able or or probably the best person to advise on or or come to answer I'm afraid. So that and how they can be improved. I'm not gonna be able to answer those, I'm afraid.

**Interviewer** 19:15  
Mm hmm. OK, that will be fine, but then. Your in your knowledge, in your opinion, do you happen to know any of the the precaution strategies.

**UPU5** 19:30  
So again, it's it's in a very overview aspect. You have this controlled by the Cyber Resilience Centre, which does a lot of that engagement with the private sector to help them either harden their targets and things like that. We know that, like I said, there's the strategies around. Protect and prepare, which you can see on…on our website and it's all about marketing and upskilling people so they can make their own decisions. The…the Cyber Resilience Centre is probably the best place to go because that is a case of I don't know what the risks are to my network. How can I go on and find somebody to help me with that. Cyber Resilience Centre doesn’t do that for you. But, it will help you with locating another private sector engagement who is basically verified so that they can help you with that aspect of doing it and helping people to define things themselves are appropriate.

**Interviewer** 20:29  
Mm hmm. OK.

**UPU5** 20:40  
So it it's it's more a case of…the track precaution strategies are making…raising awareness primarily and getting people to…to help themselves. I can't. I can't really say on the National Front, but the private sector front it is a case of that aspect. Just protect and prepare.

**Interviewer** 21:04  
OK, then let's move on to question four and the five. So 4 is what are the current cyber defence strategy? You know when when you, when you are facing this cyber attacks and what do you react to deal with this cyber attacks and also how do you evaluate these strategies? And what…what can be improved?

**UPU5** 21:36  
So we're sorry, defence strategies again, if you're looking at private sector, you would again, it's one of those ones. If there is an ongoing cyberattack, be that malware hacking and to where whatever you want to say, you would employ an incident response team. So that is a private sector department that will come, they will deploy it aspects on your network, they will isolate them out malware, they'll identify any persistence in the system and they will protect and harden your system from there.  
That would allow you to recover your systems if possible, and give you the best possible chance of restoring your company to a working space. There are a lot of.  
ICT and I incident response terms that are out there that I'm not an incident responder. In this aspect, the terminology out there I'm aware of, but I'm not going to try and explain it because I don't have a good enough knowledge to that.

**Interviewer** 22:40  
Umm.

**UPU5** 22:40  
But from our point of view, we would tend to get involved when after that point. So a company dealing with a cyber attack would employ an incident response team to do X. There are times when there are ongoing cyber attacks and ongoing blackmail ongoing this where the police get involved, but the reality is we are investigators, we are not network analysts or malware researchers or…or the specialists that are out there in the private sector to the private sector is better placed to deal with it because they have those IT specialists who will go into the network and deal with the issue and recover as much as they can. Evaluating them is…is going to be different…difficult because it depends on what point they've come in. If they've identified, let's say, someone in the. Can't remember too. In the Security Communication Centre.

**Interviewer** 23:49  
Mm hmm.

**UPU5** 23:50  
So within a company, they've got systems in there that identify malware beaconing, they will get an incident response team and to manage that, look at the network, see what's happened and recover from there. It might be that that malware hasn't started encrypting. It might be that nothing's been extracted and they can contain, preserve and remove that persistence from the network and get that person back up and running. However, if the ransomware has been, let's say, allowed to run its course and that person's servers are encrypted. Their report is going to tell you what…what happened on what the indicator compromise are to be able to…to put that together and work on securing your network. They wouldn't necessarily be able to recover your aspects and things like that. So it really does depend the evaluating on…on what they've done is very, very difficult because it really depends on when that, when that company gets them involved.

**Interviewer** 24:28  
Mm hmm. OK, then when you are investigating the cyber attack incident, do you work with, for example, cybersecurity firms to resolve this incident?

**UPU5** 25:05  
We will try so as the police we're…we're not here to...let say recover the network to get the company up to running and things like that. We are here to investigate what's happened. And we are here to bring those people to justice if we can.

**Interviewer** 25:23  
Mm hmm mm.

**UPU5** 25:24  
But we are not there to…to resolve the issues that the company has got. So when we come in to deal with something, ultimately what we will do is we will make contact with whoever's reported to police. They may not be the best person to talk to for us. So we may end up going to the incident response team or the..an IT team that's been dealing with it to get a better idea of that.

**Interviewer** 25:48  
Mm hmm.

**UPU5** 25:50  
That aspect of it is limited on how much we can do, because most companies do not want the police going on to their networks and extracting their data or doing anything on the network that might compromise their businesses. So they don't let us do that. We will try and work with people and private sector companies, but a lot of it depends on their legal teams. So if their legal teams don't want the police involved, don't want to give out material that might be what they will say is legally privileged or something like that. They may not allow the police to have the material to investigate. So we may have a crime. We may have somebody who's report it, but we may be unable to investigate because we haven't got any, any evidence or anything to work with to go and find any…any suspects. So it really does depend with companies on if they wish to engage or not. And a lot of them unfortunately, have aspects that will prevent them engaging with the investigation. So the answer to that is yes. We definitely try to, but it depends on if the…the private sector wish to work back with us.

**Interviewer** 27:00  
OK, so there are still a lot of limitation to investigate if you…you are investigating this, the cyber attack incident.

**UPU5** 27:12  
They don't say. Yeah very much of it. So we are we're limited by the amount of evidence that we've got and what we can do is…is dependent on how much that company wants to engage with us.

**Interviewer** 27:13  
Hmm OK, I understand. OK, let's go to question number 6 and 7 then.  
Do you think you can answer this question? And it's also about because we previously we were talking about the prevention and then how to react and then after the cyberattack events. In your opinion, do you know any of the ongoing current review or reflection measure of this post-cyberattacks? And how do you think about them?

**UPU5** 28:06  
Again, I'm from a public sector point of view, it's very difficult to to answer that because he again, it falls entirely into the private sector hands. Again, the Cyber Resilience Centre will help. We've got the the protect aspects that are out there that will support people in doing that and hardening their business after. But again, it really depends on if that business wants to engage with any of these measures. They're not, they're not forced to do it. There is a variety of aspects that will support their business and help. I think Police CyberAlarm is a good one where they can engage, provide their IP addresses. And there is a scanning system that will help identify if malware is being from the network. So if they pick that up, they are fed the information that says you have some malware on your network somewhere. You need to do something about it before something happens. It is one of those, those ones that. It really does depend on the on the company. It really…really does.  
We provide various different measures, most of them protect most of them, referral to other private sector companies. We can provide that…that protect strategy for hardening that target. But, it's difficult to say. Can I reflect or review them? Because it really depends on the company.

**Interviewer** 29:36  
Hmm. OK. And let's go to question number 8 and how do you describe the general awareness of cybersecurity among, you know, the general public?

**UPU5** 29:52  
Not great. It's probably the…the best one. People use things that are like passwords. They reuse their passwords continually. They use very basic passwords or something like that. They have no belief that this will ever happen to them, and not only that, they also have the belief that if somebody hacks through e-mail, it's not a big thing.  
And then all of a sudden it's a big thing when it all of a sudden your…your e-mail is compromised and your banking is compromised, and then your Facebook is compromised. Your credit card is compromised. your Amazon account is compromised. Nobody gets a cascade of issues. The general feeling amongst all the general awareness, let's say, is that it is…is just something that happens to other people. They have the…the 2FA, the password. They should be protected. That's how they see it. And for the most part, the…the more social engineering aspects of it. A lot of the times they are defrauded and bought into this because they are either engaging with somebody they think is trustworthy. Or they're clicking a link that they believe is from a trustworthy source. It's difficult to identify that, but a lot of the people around don't look into it enough to be able to distinguish from what's malicious and what's not. So at the moment, I'd say it's let's go with mid to low, it's better than in the UK. It's probably better than a lot of other places around, but it's still not a mass amount of awareness around cybersecurity and what it should be doing.

**Interviewer** 31:42  
Mm hmm. OK. Yeah. Then let's go to question number 9. And so do you know any…any of the governmental plans of cybersecurity education, you know, for the general public because you were talk, you were saying that the general public, they have the poor awareness of this. So do you know any of the governmental plans to improve?

**UPU5** 32:11  
I don't know the wider national plans. I only know that the aspects so our protecting will do various different drives and pushes at various different events to to try and get that out there. But nationally, no, unfortunately I don't have that, that overly.

**Interviewer** 32:14  
Mm hmm, that's alright. And how about? So when for example, when someone report the cyber attack incident to you and I believe that after you…you close the case, you might give them some of them the suggestion. So what are the suggestion you give to these victims?

**UPU5** 32:57  
If we take a, let's say, just a general person, not company. Again, it will be advice on using password managers, creating strong passwords. The real basic advice there to start with using two factor authentication, not reusing your passwords.  
Not giving out details. Make sure you know who you're talking to. Don't trust people online. How to spot sort of phishing links or smishing links. I've spot fraud online. What's safe and what's not safe to go to in the…the Internet environment? Those sort of basic aspects around security to…to harden that person so they won't do it again. Again, it depends on how what kind of a person they are, what kind of response they've got and where they listen.

With a company. it's a little bit more different So, there are aspects around it where they can be provided with exercises which will help board members understand the importance of cybersecurity. There are inputs for the team that help them identify phishing and security risks and aspects around that, along with improving the general stuff like passwords security, 2FA managers who you should and shouldn't pass your…your stuff onto. And a lot of that. On top of that, you've again got the…the Cyber Resilience Centres that will provide that ongoing support with.  
For example, companies we will try and get them to engage in Cyber Alarm programme that we…I mentioned earlier to give them that safety and knowledge that they if they…they do have something on their network, we might be able to spot it before it comes a problem even if the systems on the network aren't. There is another process that I think we tend to get people to engage in. I probably could find it on the on a website, but I cannot remember what it is, but there's aspects where they…they do certain things on the network to get higher rated security.  
And they get basically certifications based on the network security which might give them better confidence. So yeah, there's…there's quite a lot that's done after.

**Interviewer** 35:27  
OK. Yeah then. Then let's go to question number10. Then number 9 is about the general public. And how about the governmental plan to attract future cybersecurity talents or cultivate them? Do you have any of the and do you know any of those that the plans from the government or the public?

**UPU5** 35:55  
I don't. I'm I'm afraid that that's probably out of my area of expertise in a massive way, I'm afraid.

**Interviewer** 36:04  
Mm hmm. No, that's alright. Yeah.  
Yeah. OK then let's go to section D cause section D it's yeah, about a public private partnerships. So first question is what do you think of this idea? Public private partnerships in terms of cybersecurity, do you think that will help the whole security?

**UPU5** 36:27  
Yes, in short, that's easy answer.

**Interviewer** 36:31  
Yeah.

**UPU5** 36:32  
The public sector doesn't have the resources to do everything out there. Not only that, they don't have the skill set. The private sector does. The reality is there are volunteer schemes as well for the police. You've got cyber…Cyber volunteer schemes, Cyber digital volunteers. There we go CVS. They can come in from private sector and they provide that expert advice. On top of that, we use a lot of companies within here that provide additional support to us in our investigations. That also works backwards as well. So when it comes to public private sector, the cyber resilience sensors work with that, so as a public sector agency, we aren't allowed to advise people to go with one private sector company over another. Because we can't favourite it. We're not allowed to do that, so I can't tell you to go and use Microsoft over Linux. In that aspect, and I can't be biassed to one way or another. What we can do and what we can set up with partnerships, is work with and verify those providers that are decent, how integrity are open and honest. And match that vetting level so that people know if they are using. Those public private sectors are partnerships, especially with the CRC (Cyber Resilience Centre). They are getting something that they can rely on.

**Interviewer** 38:08  
OK. And. Question number 2 is. So now we know. You know, it's you think it's. It's good to have this kind of partnerships in terms of this cybersecurity. And do you know the current mechanisms of this cooperation, this partnership?

**UPU5** 38:34  
When you say mechanisms, what do you mean by that?

**Interviewer** 38:37  
It doesn't have to mechanism like how? So for some of them when…when we want to secure our cyber. So for some of the government or the police force. And do they work with the…the…the cybersecurity company to work with that and how do they work with each other, you know to?

**UPU5** 39:01  
So if we were working backwards in the…the…the police wanted to…to deal with their networks and things like that, then yeah, you would go through what's called…a procurement process to…to go for that. So if you're looking at any large contracts with the private sector agency, then it goes in at a procurement phase generally by the Home Office who verifies to certain suppliers. They once they are approved or…or brought in, that is a supplier we will use. There are other ways we can go about obtaining supplies, but we generally have one supply for one specific thing to bring that in. There are other means of methods, but. Again, engaging like that.  
We have that to…to drive our cyber security forward and we use that Home Office approved system to do it.  
The other aspects are that. For outside again, it is that cooperation comes with us where we can't identify. We aren't allowed to prefer one private sector contractor over another. We use again. You're. You've heard me refer to this a lot. Cyber Resilience Centre and they can advise these vetted contractors who provide certain services, be that incident response network analysis, that sort of thing. You can go and get them and pick from a pool of things there that are. There might be contractors that work within the public sector as well to provide certain aspects of it. So we know that they are vetted and we know that they are secure and you can get that on the…the private side as well as the public side.

**Interviewer** 40:48  
Mm hmm.  
Mm hmm. OK. And then do you have the experience of for example, you are investigating this cyber attack incident and then you need to access to some I don't… data or something but you don't have this kind of resource. So you outsource to the…the cybersecurity company, they help you to investigate this kind of things and.

**UPU5** 41:18  
Yeah. So the…the public sector, especially in cyber, lives on experts. So we, like I said, we're not network analysts, we're not. We're investigators. So what we will do is when we investigate if we have, let's say a huge server log that's been dealt with or something, there's been apartment attack, we will go out and seek a private sector company to review that. And go from there. And they will give us a report. They will also give us statements so that that helps us to analyse it and we can use that in material evidence. If we were to go out and get those companies, there are lists and approved suppliers of those sort of things.  
There's if it comes down to somebody providing, let's say, expert evidence in court, there are there are lists of expert witnesses out there or people who are of people who are deemed to be an expert in that field, that we can go and access.  
In relation to other aspects, there are other things we engage with. We engage with the private sector a lot around obtaining data. So if you're looking at, let's say, Facebook is a good example, we will engage with Facebook, comply with their legislation, also comply with the UK's legislation to obtain the data that we need to advance the investigation.

**Interviewer** 42:40  
Mm hmm.

**UPU5** 42:51  
If we're looking at specialist analytics. For again large scale data or something like that, we can obtain companies. There are companies that have gone through that procurement process who provide services and tools that we can go to probably additional cost to provide us some analysis or…or understanding on something like that. So we work with partners all the time.

**Interviewer** 43:19  
OK. And then have you ever encountered some difficulties when you partner up with them?

**UPU5** 43:29  
International borders. It is the easy answer to that.

**Interviewer** 43:32  
Mm hmm.

**UPU5** 43:33  
If we are going to deal with somebody, you're going to talk to somebody. You're trying to get somebody to do something for us. Many of the companies that are sort of the best, that's it, will be based in a another country. Let's pick the US for example. There are aspects around assisting the police or assisting a foreign country that have to be carefully managed for us to do that. They will work with us, but international borders pose a problem because we have to comply with legislation on both sides and also bridge those barriers so we don't inadvertently break the law.

**Interviewer** 44:16  
Mm hmm.

**UPU5** 44:16  
So yeah, there are working with the private sector in that partnership working, be it, let's say if you take my area of business, let's take someone like Binance or Coinbase. If I was to engage with them to get them to work. Need I need to comply with the legislation where they're based? If it's a company like Binance, they're based in Seychelles. So if I want data out of them, I've got to comply with the law in the Seychelles and get court orders in the Seychelles to get that data.

**Interviewer** 44:39  
Hmm.

**UPU5** 44:52  
It causes a lot of costs, a lot of time. And quite a lot of negotiation to get to where we need to be in certain aspects to get material out eventually.

**Interviewer** 45:05  
OK. And then what do you think about the future plans on this partnerships or what can be improved or what do you think it will be better to continue this partnership.

**UPU5** 45:25  
I've seen a lot of people try, but it's…it's about the police forces. Or law enforcement agencies engaging with private sector. It's very, very difficult for us because we are very hemmed in by legislation, there's a lot of rules for us to follow and things like that. We have to do things in a very specific way because there are companies out there that might not deal with that kind of legislation, might not understand or say English isn't their first language. Engaging with them and having that conversation can help move that along. It can be improved by creating those relationships with the private sector. At times, through specialist units, at times through TM rule…um…engagement. But creating those relationships will help to get it out, because although it takes not very much to create that good relationship. It it? Sorry, it takes quite a lot to create a good relationship. It doesn't take very much to destroy it. So, it depends because working across countries is always gonna be a problem. We're not gonna be able to change the laws in in one country another, I know various different countries are trying to come to mutual agreements for various different transnational, data transfers and management, things like that, but those…those laws and rules are always going to sit, so it's going to be a case of making contact with the private sector, which is…is generally back the way forward.  
I think that a very quick way for be the private sector having a more open area for us, directly contact with and talk to somebody within that private company. That would be a quick win for us, but I can also understand that in a private business you might not have, especially if you're international, you're not going to have 100 people on the phone to enter international queries from all of the law enforcement teams all over on a 24 hour basis. So, finding a balance between that somehow has to be the way forward. But yeah, everybody works at different levels and at different times and to different rules, so it makes it very, very different.

**Interviewer** 48:01  
OK. Thank you then. In general, what do you think that you know when you are having these partnerships? What can the public sec sector contribute to this partnership and what can the private sector like the private company contribute to this partnership?

**UPU5** 48:26  
So I'm the public sector from our point of view we provide. That level of security to not just the the public in general. But the company itself, it gives it that studying and that point to say we do engage with police, we are here, we are supporting, we are supporting investigations. It gives them that drive to be able to do that. It creates that positive mental attitude towards that company throughout. For them it that's going to be a benefit because the reality is if they're seen as positive company to be and if they'll see it's supportive, if they keep fraudulent elements out and hackers out and X&X&X and protect their customer base, that is a benefit for them. From our point of view, it is our job to protect that public. It is for me anyway. And keeping that aspect there and having that working allows me to investigate and allows me to take the public and recover those their their funds, their property, their whatever's been taken or whatever it is they've lost helps me to manage that investigation and bring those people to justice. It is a mutually beneficial aspect, which is why. Generally, if we work with a private partnership or a private sorry, a private company and we have engage quite heavily with them. We will offer them the chance to talk to us.

**Interviewer** 50:01  
Mm hmm.

**UPU5** 50:02  
I think one of the big ones recently that I can…I can point you at is Operation Hyphen. That is a chat which went to court in January last year, January last year, he was convicted. He created a malicious website which stole a lot of people's cryptocurrency. He was gaoled for that, convicted for that, but as part of what we were doing, we were recovering funds for victims.We worked heavily with private sector company. Know who [the name of a cryptocurrency company] is?

**Interviewer** 50:39  
Yeah, yeah.

**UPU5** 50:40  
Yeah. So we work with [the name of a cryptocurrency company] and as part of that, when we put out our media appear our media. Story Report…Media report. After [the name of a cryptocurrency company] were involved in that they said their piece because they helped out. They were able to put in their news report how much they've helped law enforcement, why they've it and what they think the benefit is. So it is that that joint working creates that stronger bond and helps protect everybody.

**Interviewer** 50:52  
OK so.  
Most of the cases you've been dealing with or the the partnership with the private company, are they most of them they are more like international companies. Is that correct?

**UPU5** 51:30  
Yeah, the the answer to that is yes, because of the way the landscape is, especially in digital environments. Most of the companies are international now, so yes.

**Interviewer** 51:40  
Yeah. OK. And so that that's why it will put more.  
Difficulties during this this cooperations because like…like you said, it will be the.  
Another country's legislation you need to comply with, so it will be much more difficult for you to deal with that.  
OK. OK. Then I think that's it. And thank you so much. So I'm going to press stop.