0:0:0.0 --> 0:0:4.50  
Interviewer  
Okay now I think, yeah, we are recording right now.

0:0:4.970 --> 0:0:5.250  
UPU3  
Perfect.

0:0:5.670 --> 0:0:19.440  
Interviewer  
Yeah, okay. So let's get started. So we are just going to start from section A for some basic information. So the first question is, which one does your unit that you work for belong to?

0:0:20.560 --> 0:0:26.30  
UPU3  
Okay so I…I do work for the [the name of the national-level police force].

0:0:27.290 --> 0:0:27.930  
Interviewer  
Okay so.

0:0:27.270 --> 0:0:29.340  
UPU3  
Which is public sector, yeah.

0:0:29.930 --> 0:0:41.530  
Interviewer  
Okay, thank you. And then, yeah, so I think you just answered the question two, but yeah, what you need to do work for like in the [the name of the national-level police force].

0:0:47.930 --> 0:0:48.430  
Interviewer  
OK.

0:0:42.910 --> 0:0:49.490  
UPU3  
And so the unit is called digital cyber and communication is with forensics.

0:0:50.560 --> 0:0:56.450  
Interviewer  
Okay, thank you. And then the third question is, how long have you been working for the unit?

0:0:57.360 --> 0:1:2.500  
UPU3  
Uh, I think coming to October is gonna be five years.

0:1:4.140 --> 0:1:4.510  
UPU3  
Yes.

0:1:2.980 --> 0:1:5.450  
Interviewer  
Five years. Wow, that's really long.

0:1:6.490 --> 0:1:12.440  
Interviewer  
In the so the 4th question, what position do you hold within the unit?

0:1:13.380 --> 0:1:17.180  
UPU3  
OK, so at the moment I'm digital forensic specialist.

0:1:18.0 --> 0:1:24.750  
Interviewer  
OK, OK. And then the 5th question, what are your main responsibilities?

0:1:26.150 --> 0:1:34.40  
UPU3  
My responsibilities are mainly analysis of data within…within complex casework.

0:1:35.500 --> 0:1:36.40  
Interviewer  
Okay.

0:1:37.70 --> 0:1:52.970  
Interviewer  
Then okay. Thank you so much. Then, yeah, that's a basic information and we will jump to section B. Yeah, you are. You are just need to answer section BCD. That's it. Yeah.

0:1:53.800 --> 0:1:54.180  
UPU3  
OK.

0:1:54.460 --> 0:2:7.90  
Interviewer  
Yeah. OK. So for section B, the first…first question is what are the major cyber attacks in the UK and what are the modus operandi and could you give some examples?

0:2:8.750 --> 0:2:16.100  
UPU3  
I would say most…most of the instances are for related to phishing.

0:2:20.880 --> 0:2:21.380  
Interviewer  
Hmm.

0:2:16.900 --> 0:2:29.870  
UPU3  
Um and basically online scams and sometimes also little bit of malwares and you know viruses, bots or ransomwares. Um, some data breaches. Don't know if you have watched the news in UK recently, but we have quite a big data breach within the police for example. So we have data breaches as well, which is not really a cyberattack…per se, but you know it's quite, quite common.

0:2:56.260 --> 0:2:56.850  
UPU3  
Um. The second part of the question is, uh, some examples is what are the modus operandi? So again, phishing how it works is literally just put..put something in an e-mail in a text something for example, the same redeem your…your money here and people will just click on it and that will link to our website or to automatical download. That will download something on your computer maybe or they will trick them to share their personal data.

0:3:38.570 --> 0:3:52.660  
UPU3  
Most of the times um…ransomwares malwares are bit different. Ransomwares will basically lock your computer and lock your access to data until you pay…and yeah, pay your ransom. And that's why…and this is why it's called like that.

0:4:1.260 --> 0:4:1.640  
Interviewer  
OK.

0:4:1.670 --> 0:4:9.980  
UPU3  
A few examples. As I mentioned some…some data breaches, then they quite increased last year as well, I think people are targeting maybe like government agencies a bit more than they were before.

0:4:25.890 --> 0:4:26.390  
Interviewer  
Hmm.

0:4:20.910 --> 0:4:30.990  
UPU3  
Um, last years we had energy bills scams. For example, when the government was giving, they were giving like part of their funding, they were given as an energy bill support, so they will send you an e-mail that looks like it's from an energy supplier. They basically say redeem here your 600 pounds coupon so they were tricker to click on that and then that will trigger basically a cyberattack.

0:4:57.220 --> 0:4:57.710  
UPU3  
And.

0:5:0.50 --> 0:5:11.860  
UPU3  
But yeah, we have like, I've got plenty of examples, but yeah, we'll say mostly is phishing and frauds related to that or as a consequence of that.

0:5:13.230 --> 0:5:18.660  
Interviewer  
OK, so then I have some following questions for you. So you mentioned the…about the…the scam about the bills, do you think it's related to the, you know like the past year since past year the bills are increasing, so maybe the?

0:5:29.920 --> 0:5:30.780  
UPU3  
Yeah, definitely.

0:5:31.600 --> 0:5:32.190  
Interviewer  
Yeah.

0:5:31.510 --> 0:5:34.530  
UPU3  
Yeah, definitely is related to that. Um…I…I didn't receive one person, for example, but I know people that they did. Yeah, it was clearly a an, a method used by criminals that they were, you know, pretended to be part of government agency because of what it was happening in UK. So definitely yes.

0:5:57.580 --> 0:6:4.930  
Interviewer  
Okay, thank you. And another question is you mentioned about ransomware, right? And then like how…like when they ask for the ransom. So how…how they…how do they expect us to pay? Like maybe through? Yeah. So for example, just this is just what I heard, maybe some of them, they expect people to pay in like bitcoins, you know, like the.

0:6:26.530 --> 0:6:35.250  
UPU3  
Yeah, I would say most of the time, of course they will choose a method of payment which is hard to track. Um…Which could be any type of crypto. Can be Bitcoin. Can be any kind of Tether or anything related to that as well. Sometimes even…even for phishing, we've seen Paypal's accounts as well and, but definitely not a bank account and details and there would be easy to track down, yeah.

0:7:2.140 --> 0:7:14.140  
Interviewer  
Okay, thank you. OK then let’s move…move on to the second question. So what are the major targets of cyber attacks in UK and what…what are the reasons?

0:7:15.570 --> 0:7:28.870  
UPU3  
Um said. We say the majority is probably a large to medium businesses. They have to be fairly rich and notorious.

0:7:29.560 --> 0:7:42.470  
UPU3  
And and that's because it's related to the reason, which is basically obtained kind of compensation for me it obtain money sometimes the compensation can be…can be personal. But is very, very rare and most of the times is to obtain money out of it…um in Bitcoin or through ransomware? Sometimes we have also proper cases where you know the victim was basically like threatened that they were released certain type of data.

0:8:11.600 --> 0:8:17.370  
UPU3  
Um, there…there is a there's been a lot of few instances of this if you kind of, uh, you know, says sexually related offences was so they were released like videos they were released…I don't know web history related to that so they but they always expect some money out of it, most of the times. That's why normally are businesses.

0:8:39.440 --> 0:8:39.910  
Interviewer  
Okay.

0:8:39.430 --> 0:8:41.510  
UPU3  
Most of the times are businesses, yeah.

0:8:42.440 --> 0:8:44.350  
Interviewer  
And then um. Do you have like, um, certain types, types of business or industry? They are easy…easily to be targeted.

0:8:57.870 --> 0:9:9.180  
UPU3  
I think it's fairly with widespread and I…I would say the opposite, there are maybe certain businesses which are not easy to target, which most of the times are…um…let's say banking systems, maybe banks and financial…financial systems. They, uh, they take care about their cybersecurity a lot and for maybe not very easy to attack. However, when they actually attack them, he also gives small profit. So it's just like, yes, they don't attack them very often, but when they attack them is usually for millions of pounds of…of profit. And there's been, I would say, last year, even the year before there's been an increase in in attacks via charities…which they…they have a fair…fairly big amount of profits but they also easier to attack than other businesses because they don't expect people to do cyber attacks on..on charities. So…

0:10:24.670 --> 0:10:41.760  
Interviewer  
So charity, they are more easily to get target like just on compared to others and like the bank and financial industry are not that easy to attack cause it's they have better cybersecurity?

0:10:42.580 --> 0:10:45.650  
UPU3  
Yeah, I was saying, in general, overall, yes.

0:10:47.220 --> 0:10:55.160  
UPU3  
Yeah, like looking at statistics. Yeah. In general, the middle businesses are the preferred attacks because they have enough profit to justify the attack, and so when they actually attack goes…goes well, they can make enough money out of it. But it's so so easier to attack them…bigger businesses. OK, so it's it's a classic is a well balanced and situation in the middle.

0:11:21.330 --> 0:11:22.610  
Interviewer  
OK. Thank you.

0:11:23.340 --> 0:11:34.680  
Interviewer  
Yeah, yeah, that makes sense. So then the third question is, what are the factors affecting the cybersecurity in the UK and you can also give some examples.

0:11:36.130 --> 0:11:39.960  
UPU3  
Um, I'll say negatively or positively?

0:11:40.840 --> 0:11:42.140  
Interviewer  
Hmm…both.

0:11:44.690 --> 0:11:45.320  
UPU3  
OK.

0:11:44.910 --> 0:11:45.990  
Interviewer  
Yeah, I think.

0:11:45.400 --> 0:11:50.640  
UPU3  
And so say OK, let's start from the negative points. I'd say budget. Budget is a factor. Working public service and budget is one of the main issues in the sense that cybersecurity is considered…um…rich environment in since even the employer the worker in cybersecurity, they have high salaries and so we struggled to find good people for this. So if you want to invest in cybersecurity for the for an organisation you have to spend a lot of money.

0:12:29.190 --> 0:12:30.930  
UPU3  
Yeah, of course that…it's justified and is preferred because…and let's say history has taught us that most of the times that they there's been an attack, the consequences or dealing with the consequences is probably worse than actually being prepared for it…spending money before to prevent the attack and so yeah, budget affects negatively, cybersecurity will say…a little bit of…understanding of what are the impact of cyber crime and cybersecurity as well. Most of the businesses that's why that is I mentioned before charities, they don't really understand how important it is to…to invest in. So in a good cybersecurity and good…um…protection against cyberattacks.

0:13:33.60 --> 0:13:35.690  
UPU3  
And so maybe a little bit…we might need to...to like to train people and to educate people a little bit more of what the cybersecurity is…and what cyber crime is…as well.

0:13:50.10 --> 0:13:50.530  
Interviewer  
Hmm. OK.

0:13:53.890 --> 0:13:55.140  
UPU3  
Yeah, I would say this.

0:13:56.190 --> 0:14:3.560  
Interviewer  
So basically two…um…points on… the 1st is budget…like they are not that willing to invest in cybersecurity, maybe? And then a second is kind of like awareness?

0:14:11.830 --> 0:14:20.780  
UPU3  
Yes, yes, um, for some, for some organisations I would say more than be willing to invest as little.  
They cannot invest or they cannot invest as much. Of course is part…over budget.

0:14:29.960 --> 0:14:30.400  
Interviewer  
Okay.

0:14:29.810 --> 0:14:46.50  
UPU3  
And…and because…because some of the industries that there are…there are stable, they don't, they never have to invest a part of their budget in cybersecurity before. Because they're not so educating them…educate about cybersecurity, they struggle to invest part of this budget. While it might be easier, for example, for us…for, you know, young startup to invest in cybersecurity because they have more awareness of what of the risk of cyber crime?

0:15:10.830 --> 0:15:11.450  
Interviewer  
Ohh okay.

0:15:13.600 --> 0:15:20.610  
Interviewer  
Yeah. OK. Thank you. Then. So it's for a negative aspect, right? And then?

0:15:20.40 --> 0:15:23.210  
UPU3  
Yeah, yeah. There's some negative aspects, I would say.

0:15:24.710 --> 0:15:28.820  
UPU3  
Positive as…aspects of cybersecurity, I would say on the other hand, for example, I say yes, people they don't have um…very deep knowledge of hat's cybersecurity is and what cyber crime is. And sometimes they always think is less of a crime than other crimes.

0:15:48.940 --> 0:16:9.150  
UPU3  
And, but I would say positive UK was to spend a lot of money, try to educate these people and try to and try to provide tools or resources or training or even stuffing sometimes. They will develop um…basically part of the organisation they will…and then go to a business and test their cybersecurity system. So I will say…it's…on that aspect, UK does pretty well compared to other country. And then there's been done late. It’s like from let's say, a few years, maybe two or three years, that this has been done more. But yeah, before it wasn’t that much as now. Yeah.

0:16:50.480 --> 0:16:52.600  
Interviewer  
Okay then.

0:16:53.280 --> 0:16:56.50  
Interviewer  
I would like to ask you more about…Do you think there will be some factors like political factors or like geographic factors or like economical factors that would like affect some security in the UK?

0:17:14.290 --> 0:17:16.380  
UPU3  
Yes, yes, definitely…um…so in terms of political factors, and… which is connected to geographical and so on, I would say depending on where you are in the world.

0:17:31.200 --> 0:17:31.670  
Interviewer  
Hmm.

0:17:31.150 --> 0:17:40.880  
UPU3  
Yeah, this is a outside UK, of course. But what you are in the world, it depends if you're gonna invest in cybersecurity or not. And in the sense that any type of Western world is more targeted than other part of the world. So for example, UK, US, Europe or businesses based in these areas.

0:17:59.170 --> 0:18:3.890  
UPU3  
Asia as well. You know, Asia especially part of Asia can be fairly rich and you know profitable for cyber crime. Um. And they will also spend more money investing in this kind of area. And so it's also be political because…um…I'm not sure. I'm not sure about this statistics about this. But, a big number of cyber…cyber criminals group…um…are based in between Asia, Russia and this kind of areas. So, most of times to conduct a safe attack, they will conduct an attack further from where they are…and…said they would probably target more certain areas of the world than others.

0:18:58.660 --> 0:19:11.60  
UPU3  
So yeah, definitely in geo…yeah, geography and politics definitely does a lot in terms of internal in UK legislations is definitely impact…as cybersecurity and…

0:19:15.920 --> 0:19:23.810  
UPU3  
They know what else is related to it, but possibly like taxes or there others stuff that can affect it as well.

0:19:25.920 --> 0:19:44.210  
Interviewer  
OK then let's move on to section C and the first question is what are the overall cybersecurity plan of the UK government that like based on what you know and how would you evaluate this plans?

0:19:45.730 --> 0:20:6.760  
UPU3  
Okay um so then I might try a couple of stuff before, but I think last year…the government released basically what's their cybersecurity plan the whole UK is and involves a lot of different aspects. Um, but definitely there is…let's say uh, like overall a summary of it…is that they want to increase awareness in people.

0:20:20.470 --> 0:20:21.210  
Interviewer  
Hmm.

0:20:20.590 --> 0:20:50.720  
UPU3  
And businesses and…and invest more in cybersecurity. And they are also trying much more to extend its appear related to awareness and where it is about. And they also tried to extend their areas of influence and so imagine you got the UK Government you got a business most of the times the business will automatically…assume that the UK government cannot help with the…with their cybersecurity department, but…yeah, well, they're trying to do is that and…

0:21:4.930 --> 0:21:9.310  
UPU3  
Basically, publicise a bit more the fact that they can help…um…in providing cy…cybersecurity to businesses as well to individuals.

0:21:17.320 --> 0:21:19.210  
UPU3  
And so that's their plan. I think it's an 8-year plan. So it's…it's gonna cover like the next 8 years. They're gonna focus a lot on this kind of aspects…And…And then the rest.

0:21:32.350 --> 0:21:34.810  
Interviewer  
Eight years, right? Eight years.

0:21:34.340 --> 0:21:42.410  
UPU3  
Um…I think so. Now on the lesson, Sheba, I believe is until 2030.

0:21:43.540 --> 0:21:44.310  
Interviewer  
Ohh OK.

0:21:43.220 --> 0:21:44.430  
UPU3  
Yeah, and…It was done last year and so…yeah, until 2030.

0:21:51.350 --> 0:21:57.400  
Interviewer  
OK. I…I can do a little bit search after the meeting, yeah, so.

0:21:56.560 --> 0:22:0.630  
UPU3  
Yeah, you won't take it. I can send it to you. God I save it somewhere…Yeah.

0:22:1.550 --> 0:22:4.410  
Interviewer  
OK, now that that would be that would be good. Yeah. Thanks.

0:22:5.620 --> 0:22:17.410  
Interviewer  
Okay then um so for the second question is um, I think the 2nd and the 3rd question can be answered together so…um…so I want you to. I want to ask your opinions about the current cyber threat precaution strategies and then how do you evaluate them and also what else can be improved.

0:22:34.380 --> 0:22:34.950  
UPU3  
Okay. And so the…the government again after this plan changed…and a few a few way of approaching and stuff while before was…let's say bit reactive, so it was and their cybersecurity, their investigations about cyber crime was always a reaction to something that already happened. And…and now there is a lot of highlights on and pro auction. So we…we tried to…to do it before. I think they have a like an approach name for this. But basically it means they are trying to when a business is created when an organisation is created, they do…they…they basically make a lot of security measures. OK, they basically and share before that they are appropriate, they are proportionate to the technology that we use, for example, because you know, we don't need strong cybersecurity or so you know as we don't need to test something for cyber crime. If we don't really use that type of technology, you know, we always test the something that can be attacked.

0:23:58.550 --> 0:23:59.40  
UPU3  
Um…But yeah, basically it's making sure everything works and everything is watertight before and then once…um…once the organisation reads started to be deployed, then irregularly checks and that's this cybersecurity stances work, and they keep doing that basically regularly, more than actually just…basically, after the attack has been as up and they tried to figure out why or what went wrong. While now we keep monitoring how…how…how our cyber defence works basically, and if it works well.

0:24:53.160 --> 0:25:3.490  
Interviewer  
And then what do you think? Uh, in what aspect do you think uh can be maybe improved or yeah to make it better?

0:25:4.400 --> 0:25:4.910  
UPU3  
Um…So I will say…yeah, probably…um, I'm not so I'm not 100% sure how this approach is done. That's the thing.

0:25:18.850 --> 0:25:45.410  
UPU3  
Um, sometimes um governmentation could be a bit out the heat, and so hopefully they will hire people. For example, for doing some penetration testings or some kind of, you know, basically heretical lacking against the company itself. I'm not sure if this is done, to be honest, because I still believe it cannot be done by someone internal to the organisation itself sometimes because it's…um…I…I don't know. I think like in terms of bias, it’s a bit hard to try to attack the…their owner organisation you work for, even if it's for a test.

0:26:7.940 --> 0:26:8.570  
Interviewer  
Hmm.

0:26:8.230 --> 0:26:21.140  
UPU3  
And so hopefully I'm not sure how in terms of staffing and who is gonna do this, how they decided to manage this. I think he has to be…reviewed, maybe. Because I know everything is done internally now. And sometimes they're very surprised when someone external is able to, you know, to bypass our security. And…But yeah, maybe should have been done by someone external.

0:26:46.420 --> 0:26:50.570  
Interviewer  
Okay, thank you then. And let's move on to the 4th question and the 5th question. So um, so previously we were talking about the precaution and now I want to ask about the when you are facing the ongoing cyberattack, um, so what is your current um like defence strategies? Or like how? Like what will you do when you are facing the attack and how do you evaluate them and then and also like what else can be improved or like advanced?

0:27:29.500 --> 0:27:33.990  
UPU3  
Well, um, so tricky question in the sense that, um…and so they the cyberattack already happened. So unfortunately you know if…if…if we are in that situation that we cannot do anything else to stop it. And I will say the only thing we can do that now is minimise the risk.

0:27:53.760 --> 0:27:54.470  
Interviewer  
Hmm.

0:27:53.840 --> 0:28:3.730  
UPU3  
And so it’s…reduce it if it's still ongoing and there is still like a data breach or something like this, we can still reduce it.

0:28:4.410 --> 0:28:5.0  
UPU3  
And…definitely will require a lot of efforts and probably money invested in reducing it. And but yeah, I think the only solution after a severe attack has been done is reduce, minimising the risks, possibly to 0. Most of the times it's not possible and so yeah, minimising the risks. I think is the only thing I can think of.

0:28:36.190 --> 0:28:39.780  
UPU3  
And how is this done? Um…well, it's done through controls, so it's very out of views of the fact with their attack. Yeah, and…and how many people has been affected, for example, if they are attacked…if it's a big business. Um…So for example, I would a couple of police forces had data breaches. Yeah, it's out of view of how many people are affected, how this affected the people that are affected and…and try to minimise every possible risks to the people itself. And which again there is cannot be…eliminated. It's just reducing, unfortunately.

0:29:28.710 --> 0:29:31.110  
UPU3  
Strategy reaction. To be honest with you… like…reaction…like…it works...good, but it's not ideal. Um, I don't feel reaction is…is already too late…is already a step too late so…and it does work, but not that well.

0:29:51.290 --> 0:29:51.990  
Interviewer  
Hmm.

0:29:51.940 --> 0:29:52.100  
UPU3  
Yeah.

0:29:52.750 --> 0:29:59.650  
Interviewer  
Okay then if it's not that, well then how do you think can be improved?

0:30:15.980 --> 0:30:21.890  
UPU3  
Um…I know I sound like a bit of descent, but I would say…possibly just…just invest more money in prevention. It would be better to invest more money in prevention and in in security and defence. And yeah.

0:30:25.920 --> 0:30:55.970  
Interviewer  
Okay. So don't worry about your answer because I…I mean, um obviously you are more professional than me, so I'm that's why I…I want to do the interview cause yeah, it's better to if that's…that's your opinion to…you know…to invest money and to…to make it better and that's that that's the answer that I want. So just yeah just let me…tell me what you know about it that that's it. Yeah. Yeah. So there's no right or wrong answers here.

0:30:59.880 --> 0:31:0.190  
UPU3  
Okay.

0:31:0.690 --> 0:31:31.40  
Interviewer  
Okay. Yeah. So thank you so much. And then let's move on to question number six and seven. So I think the six and seven is kind of related to question two and three because now I'm going to ask you about like after the cyberattacks. So you are going to have some reflection measures. So then you're going to do some reviews and I want to ask you about. Your opinions on these measures and strategies and is that good? Is that enough? And then how can you improve or advance?

0:31:45.110 --> 0:32:4.750  
UPU3  
Hmm. Um, so let's say um, so this again we…we failed in prevention and cyberattack as happened we minimise the risks as much as we could and now it's basically we are dealing with the aftermath of the attack itself.

0:32:13.980 --> 0:32:14.420  
Interviewer  
Hmm.

0:32:5.280 --> 0:32:24.310  
UPU3  
Um, well, first of all, I would say, uh, we need a big part of it is understanding what went wrong. So investigation, said first is to do an investigation and understand what was went wrong.

0:32:26.360 --> 0:32:43.710  
UPU3  
Then, when we actually understood what went wrong, for the next time, what we want to do is fixing the issue and if we have a desperation, if we have any kind of like infrastructure that is a bit…weak. Yeah, we want to invest in that.

0:32:48.690 --> 0:33:14.660  
UPU3  
Um and…and make it as much water side as possible. And of course this will, you know, imagine if you have a like a bunch of infrastructures and one is weaker than the others. Once you fix that. And now that one is the strongest, it means the somewhere else is weakest. And so technically you should try to cover as much as you can. Um, so try to fix little issues. Also in part of…uh…in parts that they were not attacked or breached. And so yeah, definitely investigation and try to fix this…this problem or what caused the attack. Yeah.

0:33:37.270 --> 0:33:37.790  
Interviewer  
OK.

0:33:38.30 --> 0:33:41.550  
UPU3  
Sometimes it can be something very, very simple. Yeah, sometimes people don't…don't understand that a lot of cyberattacks, a lot of phishing's coming. It is done in a very simple way, yeah.

0:33:53.830 --> 0:33:54.350  
Interviewer  
Hmm.

0:33:56.330 --> 0:34:2.310  
Interviewer  
OK, so it's called social engineering attack, right? Kind of like that?

0:34:4.180 --> 0:34:6.540  
UPU3  
But yeah, kind of, yeah.

0:34:7.730 --> 0:34:8.220  
Interviewer  
Okay.

0:34:7.980 --> 0:34:12.830  
UPU3  
And we want to also possibly like social engineering, we will would like to…you know the kind of replicate the attack the engine like we got an attack. Yeah. We minimise the risk. We fixed the…the issue. Now we want to do it again. To see if it actually works. That's why the government is trying to put this…If I find it, I'll, I'll, I'll send you the…the actual name of it is.

0:34:38.270 --> 0:34:41.240  
UPU3  
And they're called controls. Um… I don't remember the name, but it's…it's basically like imagine some…um…some… in some areas or so when you're dealing with your cybersecurity, you have some kind of…risky doors.

0:34:56.550 --> 0:35:6.940  
UPU3  
Yeah. So you…you check a point or stages. Yeah. You Check Point. You. You check that point. That's your door. And that if that works, you go to stage two.

0:35:7.750 --> 0:35:8.240  
Interviewer  
Hmm.

0:35:7.840 --> 0:35:18.910  
UPU3  
If it doesn't work, you fix again stage one, so you have this continuous checkpoints to…to review your cybersecurity, your Internet service security across the whole organisation.

0:35:24.800 --> 0:35:24.990  
UPU3  
And.

0:35:25.710 --> 0:35:36.70  
UPU3  
And it's fine. Imagine, you know, if he…if you talk about in a physical world. Yeah. If you have a building, you want to have multiple doors. Yeah. So there is one entry door and is not once you enter inside that you can have access to everything. Yeah, different doors with different security levels and so on. It's basically the same thing. Yeah.

0:35:50.100 --> 0:35:50.780  
Interviewer  
OK.

0:35:51.300 --> 0:36:4.420  
UPU3  
That…so if…if another attack happens, we can kind of stop it in one stage, which is not, maybe that harmful as continuously progressing.

0:36:6.800 --> 0:36:23.670  
Interviewer  
OK. OK. Thank you. Then let's move on to question eight. So question eight is about the general public's awareness on cybersecurity. So how would you describe that?

0:36:25.620 --> 0:36:33.470  
UPU3  
Well, I'm gonna use the word…um…poor or very poor. OK, poor or very poor, unfortunately. And, so…so I deal with um, with different type of crimes, for example, and…and the issue is this. In the mentality of people….the majority of people cyber crime is…I know it sounds ridiculous, but it's not a crime.

0:36:53.830 --> 0:37:16.120  
UPU3  
OK, they don't...they don't realise how harmful can be and while and, for example like yes, you might read a little bit about cyber crime attacks in the news. OK, but there are not as covered by the news or newspaper as much as violent crime. Yeah, if there is a very violent murder or a very, you know, now there's type of serious crime. And has more highlight by the news…which was affect how people thinks about it. Yeah, and while…And I think, and I don't remember which company was, I think it was one of the energy company has been attacked last year, for example. And they lost something like £500 million.

0:37:51.430 --> 0:37:51.860  
Interviewer  
Wow.

0:37:51.480 --> 0:38:13.70  
UPU3  
People don't. People don't realise how much money a single attack can…can…can results of and. But yeah, so in general there understanding of cybersecurity and you know in cyber and cyber crime among the public is poor.

0:38:13.630 --> 0:38:14.290  
Interviewer  
Hmm.

0:38:14.820 --> 0:38:17.350  
UPU3  
And they also don't realise…the results that can affect them.

0:38:21.700 --> 0:38:22.160  
Interviewer  
Hmm.

0:38:21.950 --> 0:38:27.450  
UPU3  
Yeah. And so for example, that's why phishing works a lot with…normal people.

0:38:29.690 --> 0:38:30.190  
Interviewer  
Hmm.

0:38:29.920 --> 0:38:33.210  
UPU3  
And especially if they don't have a…if they're not tax savvy or don't have a like a an academic education, you know it's they don't realise how harmful can be to, I don't know, just enter your bank details on our website you’ve never seen before. Yeah. And this kind of stuff.

0:38:56.420 --> 0:38:57.850  
Interviewer  
OK then.

0:38:58.970 --> 0:39:2.670  
Interviewer  
I think that kind of reflect to the…um…question nine. So since the general public has really poor…poor awareness, so and what are the current governmental plans of cybersecurity education for general public? like, yeah.

0:39:20.750 --> 0:39:21.580  
UPU3  
Yeah. So. So the government has put in place like a few…Hmm…a list of agencies from scratch. Yeah, and a few…and…and these agents here create a few campaigns about promoting cybersecurity awareness. So now they will uh...before, they will do some services for the for businesses about…This could be from training to a little just some…some days where they will do presentations and stuff both so they will help them build their cybersecurity awareness and. So, to be honest, I’m very happy about um…what the government is doing lately. It's not perfect. It's not perfect, but I think if it's well with prevention. Yeah, the more…more, the more people know about cybersecurity, the easier it is…to be secure. So that's how…the…the government is trying to do that but, but yeah, there are a few, a lot of tools or…and…ohh yeah, resource is available online by the government, made by the government to help people…with cybersecurity. And they're also much more present on social media than they were before. Yes, so. I mean…LinkedIn and even the Instagram. They…they…they try to.to be more present. Yeah. While before was be of a niche.

0:41:16.660 --> 0:41:23.350  
Interviewer  
Okay. So then do you think, um, the current like campaign…and are they enough? Like you said, like for example through social media. Maybe it's better than before, but are…are they enough? And then if not, how can be improved?

0:41:37.840 --> 0:41:39.610  
UPU3  
And I would say…is not enough. Um…It's probably an improvement from before and but definitely I think…even on social media, to be honest, I…there are there are present. But, it's hard to be…it's hard for them to be visible. I don't know what to say. So for example, yeah, I have them on social media and I have all these organisation on social media because I work in this department.

0:42:14.440 --> 0:42:19.590  
UPU3  
And maybe they need to start to target…on the…you know, the people that don't know about cybersecurity and which they are trying. So it's getting…it's getting there.

0:42:31.340 --> 0:42:31.890  
Interviewer  
Hmm.

0:42:32.290 --> 0:42:38.20  
UPU3  
But yeah, it's I still needs an improvement. So how to do that? Well, I guess…I guess has to be done more under our marketing maybe.

0:42:46.360 --> 0:42:49.580  
UPU3  
And point of view, which I'm not really…I don't really know a lot about it, but yeah, definitely is the way that they present themselves. I think it's a bit…no, you know, it’s still not there, yes.

0:43:5.240 --> 0:43:5.730  
Interviewer  
OK. Then the…question ten is, um, what are the current governmental cultivation plan for the future cybersecurity talent and maybe in school or outside the school?

0:43:21.290 --> 0:43:27.790  
UPU3  
And well, this is kind of connected to the…the question, the answer before. Um, because one of the…one of the effects of the…this kind of plans that they have for a, for a educating people and those for train people in cybersecurity, there are a bunch of bursaries and you know for…for the grace. So they help people to study they…they might provide some scholarships, they might provide some…some internal…uh, stages.

0:44:7.50 --> 0:44:11.20  
UPU3  
And the basically like some…some kind of opportunities. That they are trying to attract young people, especially students. Yeah, to do so.

0:44:21.640 --> 0:44:24.310  
UPU3  
But they're also trying to um…diversify a bit the people they're working for cybersecurity. I mean, you're a woman. You will understand that but…yeah, they are trying. For example, if you are, if you're a woman, they might…and you know, it's highly suggested basically and then encouraged for you to apply for a cybersecurity degree. And so yeah, they're doing quite a lot under the university aspect…of the this.

0:45:1.220 --> 0:45:4.850  
Interviewer  
Okay. And then do you think that's enough? To attract the talent or to cultivate them.

0:45:10.150 --> 0:45:10.840  
UPU3  
Um. It's good, it's good. Um, it's hard to say it's enough now, because when you're talking about education, education has very long term effects.

0:45:23.820 --> 0:45:24.880  
Interviewer  
Hmm.

0:45:24.460 --> 0:45:45.940  
UPU3  
In the sense that if you train and give someone like the degree now and they will start to work in cybersecurity and then they will become, you know, very good at what they're doing, you will see the results in five years, ten years, maybe even more. Sometimes if you act from high school onwards.

0:45:46.500 --> 0:45:55.870  
UPU3  
Um, so yeah, it…it's hard to…to review…to evaluate at the moment. I think there is the…one of the best way to go forward because….And especially young people, they…they are the ones that provides the best insights, sometimes. You know, they have creativities and a bunch of other skills that it might be very useful to cultivate.

0:46:20.20 --> 0:46:22.260  
Interviewer  
Okay then how about…after the…education. I mean, after you graduate from the uni. So you are you are now working. And if you want to improve your cybersecurity, maybe skills or awareness? And does the government have this kind of plan to train them?

0:46:44.350 --> 0:46:48.740  
UPU3  
Yes, yes. Yeah, yeah. They focus a lot on… And on new recruits, basically new students. But yes, there is…there is a lot available online and they provide even some, even some crash courses. You know, just awareness videos, you know courses that they can be like couple of hours long and they give you an insight of what phishing is, what malware is. Um, so yeah, it's…it's that is available. It's actually very useful, yeah.

0:47:25.810 --> 0:47:38.260  
Interviewer  
Ok. Then thank you so much. Then that's move on to section D. So section D is talking about the public private partnerships. So the first question is…What do you think about the idea of public private partnership in terms of cybersecurity? And does that really help?

0:47:48.920 --> 0:48:1.630  
UPU3  
I would say it's good. Um, it's um, it's fairly good point. The only problems in the sometimes there are in this kind of…um…government, you know, public and private government and contractors partnerships is that…depending on what the government is dealing with.

0:48:16.160 --> 0:48:16.480  
Interviewer  
Hmm.

0:48:16.330 --> 0:48:22.860  
UPU3  
And the security of it might creates an obstacle, of course. So sometimes, it's...it's nice to have someone to rely on, but sometimes that they cannot rely on other people. So he can be a bit difficult sometimes to…to work…and to work together with our contractor.

0:48:45.970 --> 0:48:46.520  
Interviewer  
OK.

0:48:45.850 --> 0:48:50.390  
UPU3  
And in general, we…we do it, we do it already and it does work…not perfectly again. But we do it.

0:48:56.600 --> 0:48:57.590  
Interviewer  
OK then…then what kind of the cooperation mechanism that you are carrying out right now for the private public partnerships?

0:49:11.70 --> 0:49:20.360  
UPU3  
Um, well, cooperation. Um, it works under contracts at the moment in the sense that we…um…to be honest with you, no, not so better expert about how contracts works, but…um…imagine they…they open, they open up position for a contractor with this organisation. You guess a few agencies applies and then…and evaluation happens, and they decide which one to con…contract out. But the moment on our side for what I see is that…um.

0:49:56.570 --> 0:50:9.0  
UPU3  
Basically, we have some work we need to investigate cyber crime or we need to…to do like a new evaluation of our cybersecurity defences. So we…um, we hire…back the contractor and they do a service for ourselves…and we paid them for this.

0:50:21.510 --> 0:50:28.720  
Interviewer  
So the…the private sectors you are talking about is um…are they cybersecurity firms?

0:50:29.900 --> 0:50:37.560  
UPU3  
And now it really depends on any kind of government organisation. So if you think about, I don't know…and HMRC for example, you know the company for the taxes, yeah, they…they have contractors they have, maybe they might have more than one and so they might have like four or five contractors, maybe they do different…and different tasks so they will go back to one of them and say we need…an evaluation on this aspect, on how possibly that data breaches happens on in our organisation. And they will basically give them an estimate on…on the time there is required so the contractor will go back to the organisation and say…I need a week…um…for…for doing this and they will cost this much. And they basically in for a little brief moment, the government organisation…acts as a private, so it's a conversation private to private, where you pay some money to a company to come and do a service for you.

0:51:56.60 --> 0:52:15.790  
Interviewer  
OK, then what do you think of the? What are the advantages for this cooperation between public private sectors, for example, like what can private sectors contribute to this and what can public sector contribute to this?

0:52:16.820 --> 0:52:17.750  
UPU3  
Ohh well. I think on their hand there is some kind of mutual learning from both parts and…So on their hand they…um…they have a client, which is a very, very big client, and so it's gonna they…they learn how to deal with the big cases, maybe large amount of data and so on and on our hands we see how…how an organisation…um…how different organisation works.

0:52:56.0 --> 0:53:5.710  
UPU3  
And you know when…when dealing with this kind of tasks, which I told you like, sometimes it doesn't happen because we try to do it internally. So we…we get used to work for ourselves by ourselves, so it…it's nice to see some sometimes out how is the world outside the organisation and how they do deal with it.

0:53:22.920 --> 0:53:25.210  
Interviewer  
You have a different insight maybe?

0:53:25.640 --> 0:53:27.70  
UPU3  
Yeah, yeah, definitely.

0:53:28.80 --> 0:53:30.470  
Interviewer  
Then how about the difficulties?

0:53:31.930 --> 0:53:36.760  
UPU3  
Uh, difficulties is that sometimes we work. And we work on different procedures and different standards procedures. So sometimes if we have a process in place. And their process doesn't…doesn’t fit into us, you know, the kind of collides and then…we…we are in a clash. That one point nothing works because…we can't really go against our the our same own process so and they cannot do the same and sometimes it just hang there, yeah.

0:54:18.470 --> 0:54:20.400  
Interviewer  
OK then….umm in...in what aspect can be improved if you want to continue this private public…um…partnerships in the future?

0:54:37.170 --> 0:54:37.840  
UPU3  
Um…I think…a lot more communications. Uh, definitely. Between the parties…um and communications in the sense that communication for cooperation.

0:54:53.420 --> 0:55:5.60  
UPU3  
And a lot of times there is a little bit of resistance, um, and this is totally unrelated to cybersecurity and you know, but…because…because we are a government agency, they are the private contractors and sometimes it creates a bit of clash between…there is ourselves and there is them.

0:55:32.360 --> 0:55:33.80  
Interviewer  
Hmm.

0:55:22.70 --> 0:55:35.440  
UPU3  
So they they when you got these two opposites, it's hard to cooperate and sometimes it creates a bit of personal resistance and psychological resistance between the two. And. But yeah, hopefully with a little bit more communication trying to understand that we are all on the same boat and we're all trying to work for the greater good. OK. Yeah, bit more cooperation.

0:55:55.170 --> 0:56:0.940  
Interviewer  
OK then, um, how do you think can improve their…um…willingness to cooperate with you?

0:56:7.970 --> 0:56:8.420  
UPU3  
Ohh. Good question.Um…I would say…probably being a bit more visible, present, um, communicative as well. So for example sometimes…um…they don't have a lot of um, they don't really know who we are…and don't really know what we do and we are not really, one say we're not nice people, OK? But like we hire them to do a job, they might come in. They might say they might, we might hold them…and okay just do it and let me know when it's done. And then disappear. It is not nice way of working together. OK, so definitely it'll be more of…and be more presence. I think it would be nice.

0:57:6.880 --> 0:57:11.710  
Interviewer  
OK, so it could be the trust issue. You need to gain their trust?

.

0:57:12.500 --> 0:57:14.230  
UPU3  
Yeah, definitely. It's fine. Yeah.

0:57:13.910 --> 0:57:15.900  
Interviewer  
OKOK interesting.

0:57:17.510 --> 0:57:23.740  
Interviewer  
Yes. So now just trust, do you think of any other factors?

0:57:25.830 --> 0:57:26.490  
UPU3  
Hmm. Some trust…some. Yeah, said some. Some kind of separation between government and non-government agency creates some issues sometimes.

0:57:40.890 --> 0:57:41.480  
UPU3  
Um. No, I think I think at the end not so much because…All the times I had to deal with the privates, private contractors and private contractors, staff and…you know, people wise.

0:58:4.120 --> 0:58:4.510  
Interviewer  
Hmm.

0:58:1.480 --> 0:58:19.850  
UPU3  
They're very similar to us. They like what we do, they do what we do. Um, but they just there is this thing that they work for someone else, which is a bit of a, you know, it's like working for a competitor…Yeah, they…

0:58:20.210 --> 0:58:21.500  
Interviewer  
OK, got it.

0:58:20.800 --> 0:58:24.460  
UPU3  
It creates this kind of, uh, this kind of…yeah…psychological resistance sometimes.

0:58:27.890 --> 0:58:28.480  
Interviewer  
Hmm.

0:58:28.980 --> 0:58:30.690  
UPU3  
You're working for the enemy…yeah.

0:58:32.170 --> 0:58:43.680  
Interviewer  
Yeah. OK. That's really interesting angle. So yeah, basically they are…think…they are viewing you as a enemy like rivals? So maybe they are not willing to share.

0:58:42.300 --> 0:58:45.630  
UPU3  
Yeah, right…rivals...enemies…yeah, rivals.

0:58:45.330 --> 0:58:45.880  
Interviewer  
OK.

0:58:48.150 --> 0:58:55.440  
Interviewer  
OK. Then I think that's it and you offer a lot of information. So thank you so much. Yeah.

0:58:56.830 --> 0:58:56.960  
Interviewer  
Ohh.

0:58:55.180 --> 0:58:59.330  
UPU3  
Ohh, you're welcome. You're welcome. Hopefully without too much blubbering.

0:59:0.80 --> 0:59:0.470  
UPU3  
That's.

0:59:0.10 --> 0:59:0.850  
Interviewer  
And now it's it.

0:59:2.670 --> 0:59:6.620  
Interviewer  
Yeah. Now it's, uh, yeah, it's it's a lot of information, but let me just…press stop.