**Interviewer** 0:44  
Alright, so let's get started.  
So I will start from.  
Question in section A for the basic information.  
OK, so for the first question.  
I will put you in private cybersecurity providers 'cause you have the the.  
Plenty of experience on this cybersecurity manager roles in the private business.

**UPR3** 1:16  
So so so.  
Sorry, you're you're breaking up your Internet connection or mine one of the others is just a bit poor. Maybe maybe try turning your video off.

**Interviewer** 1:23  
Oh, OK.  
OK.  
Camera.  
Umm, how about now?

**UPR3** 1:41  
Yep, sounds good.

**Interviewer** 1:42  
OK. Can you still see me?

**UPR3** 1:45  
Yes.

**Interviewer** 1:46  
OK, I don't know why, but OK, that's guess I so let me know if there there's some point you can really hear me. OK. OK. Thank you. So I will start from you know, Section A basic information. And for the first question, I will put it in private cybersecurity providers since you are always doing this cybersecurity manager in many private businesses.

**UPR3** 1:57  
Yes.

**Interviewer** 2:17  
OK. And so then question number 2, what unit do you work for right now in your company? Yeah.

**UPR3** 2:18  
Yep.  
What? What? What are in it?  
What unit?

**Interviewer** 2:31  
Sorry, can you say that again?

**UPR3** 2:34  
It so which department you mean?

**Interviewer** 2:36  
Yes. Which which department yes.

**UPR3** 2:39  
I.

**Interviewer** 2:42  
What do you mean?

**UPR3** 2:44  
It information technology it.

**Interviewer** 2:47  
Oh it. Sorry. Sorry. It's just a…IT information. OK. And number 3 is, how long have you been working for this IT team?

**UPR3** 2:49  
Yeah. And this one only about 10 months.

**Interviewer** 3:02  
10 month, OK. And. So let me just change a little bit of the question because I I can see you have…working for many businesses and but working as the…the IT role. So I want to ask you how long have you been working, as IT manager, you know in this role.

**UPR3** 3:32  
I don't always work in it. It's some information security or cybersecurity doesn't always sit in IT. So some companies I've sat in finance, some companies I've sat in legal. It just so happens I now sit in IT so I don't see my job as an IT job, so to speak. But I left the police probably about 15 years ago and I've been in some form of cybersecurity management type role, so 15 years.

**Interviewer** 3:35  
Mm hmm. OK. Mm hmm. OK. Then. When you are working as a, you know, so let me asks you about the period when you are not working this IT but for more like cybersecurity manager role and what is your main responsibilities. What are you? Yeah.

**UPR3** 4:22  
To. The main main is to protect the confidentiality, integrity, availability of the company's networks systems. So it's the, it's the, it's a stock phrase CI…you're familiar with the CIA triad?

**Interviewer** 4:35  
OK.

**UPR3** 4:41  
You fully with that?

**Interviewer** 4:43  
Yes. Yeah, the triad.

**UPR3** 4:45  
Yeah. The CIA. Confidentiality. Yeah. So it's…it's to do all of those things. Or in summary, to protect…protect the company from cyberattacks is kind of, you know, summary as well I guess.

**Interviewer** 4:55  
OK, OK, I see. So then let's go to section D. OK. And sorry because I just want to mention that I'm studying criminology, so it's more like a social science study. So some of the techniques jargon I might not that familiar with, so I will, OK.

**UPR3** 5:13  
OK. OK. Fine, good, good, good to know. I I won't use them then, OK.

**Interviewer** 5:23  
OK. Thank you so much. So section D now question, sorry it's not section D, section E, so section E the question number 1 is what are the major cyberattacks in the UK and what are the modus operandi and could you also give some examples?

**UPR3** 5:44  
OK, so the main threats rather than attacks, I tend to think about threats. So social engineering, which is phishing, smishing and vishing, so they're using, you know, overcoming human controls is probably the key threat. We probably have thousands of those every day…in every company I've worked in. So that's probably the key one. The next one is kind of probably malware. Obviously malware attacks are very common. We have malware attacks every day. Most of those threats are mitigated every day on the occasion, some attacks may get through. You may have an infection, that infection may lose…lead to the compromise of credentials. Those credentials could then be used to do whatever those credentials are used for. So that's kind of malware. Unauthorised access is another threat that would call that. So social engineering, malware and authorised access. These are the key ones on my kind of threat radar. And probably the key one at the moment is probably third parties, so third party risk around maybe one of our suppliers being compromised and then the…the…the subsequent consequence and the impact of that service going down that leads impact to us. So they're…they're kind of the core ones on my threat radar.

**Interviewer** 7:16  
OK, so the major 3 are social engineering and malware and unauthorised access.

**UPR3** 7:24  
Yeah, I mean, you can put ransomware, you, you, you could put ransomware down there as well. Yeah, yeah. Or…or make or…or ransomware and extortion, cyber extortion. So it's where somebody does compromise credentials, they may gain access to a system. There is no ransomware, but they may do a ransom demand to threaten to release the information they've stolen. So that cyber extortion. And what we're seeing is less ransomware, less technical ransomware because of what's going on in Russia and Ukraine, because that's added to a lot of disruption in the ransomware infrastructure. So we're seeing a decrease in technical ransomware and more of an increase in…in kind of cyber extortion. So unauthorised access to steal data to then ransom and to threaten that data being released. So we're seeing a bit of a shift in…in that space.

**Interviewer** 8:14  
Mm hmm. OK, that's an interesting angle when you talk about the shift of the. Yeah, the threat. And so...

**UPR3** 8:24  
It's 'cause when…when I, when I talk about threats, I…I also consider the geopolitical space and how that influences the cyber domain. You know, we do see lots of nation state-based attacks, but you know it's more reconnaissance. You know, they're not actively harming industries, they're more looking for information. That's…that's…that's the key to, you know, kind of a nation state is being able to, you know, gather the credentials, the systems and then use them when they want they want to. The nation states are more information gathering primarily.

**Interviewer** 8:56  
Mm hmm. OK, OK. OK. Thank you. Then question number 2 is, what are the major targets of the cyberattacks in the UK and also what are the reasons?

**UPR3** 9:14  
Retail businesses probably quite large and that's probably because the groups behind that probably largest group, is like organised crime groups, or individual loan actors who are looking at compromising credentials to commit fraud and what have you. So I think organised crime probably represents the greatest threat to the UK from that side of…of things and retail businesses. Businesses that sell, you know that have lots of card details and…and you know lots of lots of lots of information.  
The healthcare sector is being hit quite a lot. That's not necessarily because they're a target, it's because they are industries that focus more on care and spend their budgets based on care, not on technical security controls. So it's just that they're more vulnerable. You also see the education sector again, that's another sector where….You know, a lot of companies are run by teachers or a lot of the companies are run by health professionals and they focus on care or they focus on education and then they forget. They don't forget, they don't, not even aware of it sometimes. So there are certain sectors that have been targeted. They're not being targeted. It's more, you know, a criminal iced. When I was in the police, you know, a criminal wakes up in the morning. Over night time he would deploy all of his scans, all of his tools, and he'll come in the morning and he'll look at his computer and he'll say I've got an infection over there. I've got another infection over here. I've got some account details that are compromised over here. And then he decides what he's going to do. Now, he's not targeting what he's doing. He's not sitting there going. I'm going after that sector. What he's doing is I want anything and everything. Some of it will be of interest to him. Some of it won't be. So that's kind of what you know, that's the kind of the criminal mindset is that they're not always targeting, you know.  
That, that, that's not kind of how they do stuff. So yeah, I…I but organised crime groups will generally try and gravitate towards where the information is. And you know that's…that's it. And there are, as I said, some industries that are more susceptible, like the government, government sectors are more susceptible as well because they've not had the budgets in the past to be able to pay for cybersecurity, you know, in the recognition of the cyber threat has probably only kind of really grown, you know, over the past ten years and has been amplified by Russia, Ukraine type scenarios and stuff. So.

**Interviewer** 11:52  
OK, I see. And then how about what are the?  
Major motivations behind 'cause I can see maybe the retail business is more for like financial gains and other like healthcare sectors and education sectors. When you mentioned about them they are more like because they are more vulnerable to the cybersecurity…cyberattack. So maybe that's why they are easily to get targeted and so can you tell me more about the motivations behind?

**UPR3** 12:25  
I…I…I…in my experience when I was doing cyber crime in the police, in the private sector, the primary motivation. The most crime that's out there is acquisitive financial crime, every angle, whether it's targeting the health sector to conduct cyber extortion, whether it's, you know a different, you know, organisation because they have data. Generally, the motivation is the, you know, most crooks are very good at realising the value of data. You know, they may steal a load of data on an on an underground forum. One minute. Let me just take this. Hello. Hello mate, can you call me back in in about half an hour, would you mind? Lovely. Cheers, mate. Thanks, bye.  
Sorry.

**Interviewer** 13:14  
That that's alright.

**UPR3** 13:17  
I've got lost my phone. Now, where was I?

**Interviewer** 13:22  
And you're saying the Motivation's behind is more like financial?

**UPR3** 13:26  
Oh yeah, the motivation for probably 90% of attacks that I've ever dealt with is financial in, in, in nature. You may see some, you know, more nation state reconnaissance gathering. You may see some loan threat actors conducting denial of service attacks. You know, during the summer holidays, for example, you know, when I was in the police, we used to see a big increase in cyber attacks. That's because children were off school and they were bored, you know, so they're…they're kind of, they're a kind of seasonal cycles, you know, depending on, you know, what, what, what's going on in the world? It's the same in Taiwan. You know, you'll have public holidays you'll have school holidays and you'll…you'll see during certain seasons whether it's tax season, whether it's bonus season, whether it's, you know, religious holiday, you'll start to see themed phishing emails, malware themed and stuff. So it's all very but, but majority of it's financial in nature.

**Interviewer** 14:28  
OK. 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.

**UPR3** 14:41  
So what are the what? Sorry. What's the question, sorry.

**Interviewer** 14:45  
What are the factors affecting the cybersecurity in the UK?

**UPR3** 14:51  
What are the factors affecting cybersecurity?

**Interviewer** 14:59  
And for example, I think you just mentioned about the uh geopolitical issues or maybe some economic issue or maybe the awareness.

**UPR3** 15:08  
Yes. Yeah, I I, I, I see what you mean. Yeah. So I think it's. Yeah, general awareness of the of the of I think it's quite poor people just don't realise the potential impact of a cyber attack on an organisation. It…I think it still feels like sci-fi to a lot of…a lot of people. People are so focused on their own, you know you know, roles whether it's you know marketing or finance and what have you that you know security is…is…is something far removed, so I guess that's…that's one factor. You know. Most attacks that the UK suffer from primarily come from abroad. They won't come from the UK, the UK criminal population is not very technically savvy, you know they're not a…as…as able as you know, kind of Russian crime groups, Southeast Asian crime groups, you know, Brazilian, you know, kind of crime groups. So a lot of the attacks, I would say that probably again, that 90 plus percent of most of the attacks that will suffer from will be external. So actually a lot of the attacks sometimes will depend on the economic situation in another country. You know, countries that speak English, countries that have good infrastructure, good broadband are more likely to be targeted. When I was in in the police, we dealt with a we're dealing with online banking crime group and they were attacking every country in the world apart from Japan because they didn't have a connection in Japan who spoke the language. So language is a big barrier. Or a facilitator for criminology as well. So the fact that we speak English in England is a factor. The fact that, you know, we have, you know, a fairly good economy, you know, we…we are a fact. You know, why attack? Why attack Africa? You know they won't have as much infrastructure. A lot of the people are not going to have money in their accounts. Some of them might not speak English. They may speak more regional African dialects. So it makes the challenge, you know, more difficult. So yeah, I think economic, you know. Economic kind of, you know, importance of language. Infrastructure, good Internet speed. And yes, susceptible sighting that you know that believe, you know, believe, believe stuff so yeah.

**Interviewer** 17:34  
Then let's go to section F and section F for the question number one. I think I'm going to change a little bit of that and so I want to ask like what techniques or services that you provide to you or either for the private business you are working for or before when you…you are a police officer and so in terms of cybersecurity, what are the major services you provide.

**UPR3** 18:08  
So I I I I breakdown my services into 5 themes which is predict, which could predict prevent, detect, respond, recover for their five kind of pillars that I would use. Under predict, the primarily piece under there would be cyber threat intelligence, threat management. So that's about understanding what's going on the outside world and making sure we…we are aware of what's going on. So that's predict. Prevent is about…maybe risk management department having a risk management team, an advisory assurance function that provides advice and guidance to the business on controls they need to put in place with regards to specific projects. The prevent strand can be quite long because you know you could probably even put in red teaming…um…penetration testing. There's lots of preventative initiatives that you could put in. So predict, prevent, detect. So detect is about technical detection, about making sure that we have, you know, a good understanding of all of our estates and that we have facilities in place to…to find bad stuff on our network. Also, to make sure that we do…sorry under training and awareness, I'd also put that under predict and prevent. But again, under the attack strand that's about training and awareness because we want more people to report stuff to us. So that's what I call human detection. So technical detection and human detection, that's kind of how I like to break that down. So predict, prevent, detect, respond. That's about crisis management. It's about how we prioritise. Priority 12345. That's the kind of the 999 or the 911 service type things that's respond. And then the recovery piece is about business continuity and about all of those different kind of backup regimes, disaster recovery and stuff like that. Now all of those things working together well, there are handoffs for each kind of like each…each…each area. And what you should get at the end of that is…is a more resilient organisation, which is what we're looking to do is to strengthen our defences and become more resilient. So it's cyber resilience, I guess is kind of the output of a cybersecurity model.

**Interviewer** 20:34  
OK, cyber resilience.  
OK. Then the question number 2, I don't think that that is for you because it's it I want to ask, who are your major customers? But I don't think that.

**UPR3** 20:51  
I thought so.

**Interviewer** 20:53  
The question #2 is, who are your major customers? But I think that's not really for for you, right? The question. So I'll yeah, so I'll yeah, I'll just skip.

**UPR3** 21:02  
No, not really. I don't think it's so. Yeah. Yeah, skip that one though.

**Interviewer** 21:08  
Yeah. So then number 3 is.  
So number 3 is talking about customers as well, but I will change it a little bit. So what are the major reasons, you know, when you're providing this cybersecurity services, what are the reasons when they come to seek your advice or services?

**UPR3** 21:33  
What are the reasons? Yeah, it could be they…they want some advice on advice and guidance on a particular project. They may need they support with a an investigation into an employee perhaps. It could be in relation to a security incident that they're concerned about, it could be about somebody technology requesting more information on a specific threat to help them make a more informed decision about how they go about building a particular product. It…yeah, it'd be about policies that we have, you know, what do we need to do in all these different areas and stuff. So yeah, kind of a wide variety of…of stuff that generally align to the predict, prevent, detect, respond, recover everything. Yeah. And that's how we deliver our services is that we deliver. We deliver those through…through the team.

**Interviewer** 22:27  
Hmm. I see. And then let's go to question number 4 and number 4 is so in what aspect do you think that, you know, among the private businesses you are working for or the general public? So in what what aspect do you think that are insufficient the most, they are insufficient the most in the field of cybersecurity?

**UPR3** 22:59  
What's the most efficient?

**Interviewer** 23:01  
Uh. Insufficient, like maybe the knowledge or maybe some technology they…they are lacking of, like insufficient.

**UPR3** 23:14  
Who? What? We mean companies.

**Interviewer** 23:16  
Yeah.

**UPR3** 23:16  
Oh. Oh, no. OK, so so, so. So what do what? What organisations in the UK are lacking certain elements.

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

**UPR3** 23:26  
OK, so some regulation I think is a big issue because what…what happened, you know, when cyber crime, you know, began in the UK, I was around when that was happening, quite sadly. But there we go.  
They they targeted high risk sectors, understandably, and they made sure there's regulation for critical national infrastructure. But what? What? What? That's what that's done is. It's strengthened 1 area of our sector, but it's weakened another because, you know, if you spend a lot of money and you highly regulate a specific area, what happens is criminals will then go to the softer targets that don't have regulation. So I think if I was looking at, you know, I think that's the problem in the UK as a whole is that you know we have finance critical national infrastructure who are, you know got good budgets. They've got high regulations, spending lots of money on it, but then all the other sectors that don't fit that don't have anything, you know, there's nothing really driving them, you know, to…to kind of to kind of to…to do that. So I think regulations is, is, is one of them. Yeah, budgets of security is expensive. You know, smaller companies just can't afford it, you know, especially a young, growing company, you know, you, you'll take the risk. You're not going to spend all your money on security if you're trying to set up a new company. So it's it's…it's having that kind of balance. I don't think the technology companies that we that we use like Microsoft or Amazon, I think they're getting better, but they're not doing enough to protect customers. I mean, Microsoft's perspective used to be, you know, you buy my tool, you do your own security. We're not going to tell you what to do. You will have to bring another consultant in, spend hundreds of thousands of pounds on. Well, now what now? What do I do with this? And then they advise you. So you just have all of these. You just spending money on…on stuff that Microsoft should have a default secure. You know, rather than turning security settings on, we should be or…sorry, rather than turning, you know it should be out-of-the-box. Should be all security settings are in place and then you turn them all off. Or the ones that you don't want rather than what they do today is that it's nothing's on. You have to decide yourself. But there should be an out-of-the-box best practise. This is what we recommend. Default set.  
But they don't do that yet. I guess the technology's not there, the budgets, the regulations not there and again you know the appetite, the understanding, the awareness you know is not there either. You know people don't realise what their you know they're…they're kind of defending against and what the risks are.

**Interviewer** 26:18  
OK, so most of the reasons are regulations, budget constraint and maybe the awareness they want to…the knowledge, I mean the knowledge awareness.

**UPR3** 26:31  
Yeah, yeah, yeah, yeah.

**Interviewer** 26:32  
Oh, OK. Thank you. And then question number 5 is, so when you are providing this services and what are the common cyberattacks that you are that you have been dealing with?

**UPR3** 26:50  
Mainly unauthorised access.  
So yeah, maybe the use of malware to gain access to usernames and passwords.  
And then the compromise of those passwords on different sites, maybe a marketing site that we have. That they then use to conduct phishing again, financial motivation. So unauthorised access, social engineering, you know, quite common. Gaining access to Office 365 mailboxes. And what they do there is that they…they intercept communications with finance, pretending that they've that they're…they're an employee, they're having a conversation with finance, and then they convince finance to change the bank details on something and get them to transfer money to an account that the crooks control. So you're unauthorised access, social engineering, malware at the top, the top three attack types.

**Interviewer** 27:48  
It's an authorised access and social engineering and malware?

**UPR3** 27:53  
Yeah, unauthorised, yeah.

**Interviewer** 27:54  
Oh, OK.

**UPR3** 27:56  
It's called it's. It's also called hacking. Gaining access to a system where you don't have the authority to do it.

**Interviewer** 28:02  
Mm hmm. OK. And then let's go to question number 6. So the question is, when the cyber criminals breakthrough the defence, you set, you know, when…and then So what a mechanism for harm reduction and incident management?

**UPR3** 28:25  
So the the the key defence I think I mean the security when you look at security, they have it's what's called a layered approach. You…you know you have kind of firewalls, you have you have lots of different things in place. However, when they do get in we have what's called an EDR solution endpoint detection response and what that does is like a little security guard who sits on every single computer, every single server.  
And says….Is this normal behaviour? So it uses kind of behaviour analytics. It's using a bit of AI and it says…Is what going is…what's going on normal? So that that is you know that is the key defence put that in with…with…with antivirus as well. Put that in with web defences so you know if you try and visit a website on a fit with phishing e-mail and you click on it the web, a web proxy they call it will block…will block the website to stop it being downloaded the malware. So they're…they're…they're key defences. Once the crooks are in, endpoint detection response and for me that is a must have for every company today. And there's a lot of companies still don't have it because the threat is has moved significantly. Antiviruses is dead. It's…it's it doesn't do as much as it used to. It used to be quite important. Nowadays it's just not. It's it only deals with what's called signature-based malware or signature based which is it will only block what somebody has seen before. It doesn't block what somebody created yesterday because you know they can only blocks when it knows.  
So yeah, EDR by proxy, key…key kind of defences.

**Interviewer** 30:12  
OK. Thank you. Then question number 7 I want to ask that how do you describe?  
Or evaluate the cyber resilience of the, you know the business sectors or the public sectors, you know the governmental organisation or either the the the business, yes.  
How do you describe their cyber residence and also how can you? When you are providing your services, how can you enhance this aspect? The cyber resilience?

**UPR3** 30:51  
So cyber resilience is difficult to quantify, so you have to use KPIs, key performance indicators or KRIs, key risk indicators. So these are statistics that you will…you will have on a monthly basis or weekly. How do you want to do it, things like how quick do I take to remediate a security incident? How quick does it take me to detect a security incident? How quick does it take me to…to do whatever's next? So what you do is you get KPIs and you start off with a baseline and you understand. Well, this is where I start. If I become good at these things, I'm becoming stronger as an organisation. Strength, resilience is the same word. And you know, you use these factors. So with them…so we do lots of phishing simulation exercises, so we'll send out 10,000 fishing emails and then I'll look at the statistics of how many people open those emails, how many people reported those emails, and then I have two figures, which is the susceptibility level and the reporting level. Now if we do two of those things well, we're becoming stronger. So it's it's a way of using numbers as a mechanism to quantify strength and that we're getting better. And you could, if you wanted to, aggregate all of those numbers into one figure and call it resilience. If you wanted. I've never done it, but you could and you could use that and you know, use that as a benchmark.

**Interviewer** 32:35  
OK, so that's how you kind of quantify this cyber resilience?

**UPR3** 32:42  
Yep.

**Interviewer** 32:42  
And. Then. So then let's go to question number 8, so question number 8, 9, 10 is more about the services you provide, so I want to ask. So among the techniques and services you provide, in what aspect do you think are still insufficient and you want to improve.

**UPR3** 33:12  
Technical assurance I think would be one of them. Understanding. Or having a good handle on you know what? What security technology do we have? Is it turned on? Sometimes these things are not turned on. Sometimes companies buy lots and lots of security solutions and don't use them, or they've been turned off for whatever reason. So yeah, technical assurance about having you know, somebody that can make sure on a daily basis, everything's working as it should be. If there is new functionality within a product that that is activated and turned on…is…is one of them. So technical assurance. The other part is probably risk management. You know, working with technology under the members of the business to help remediate risks that we know and there's a plan in, in, in place to deal with them. So they're kind of like two areas. I think the recovery piece as well is…is an element. I think because people are now moving to to the cloud, they believe that recovery isn't their problem anymore. So yeah, so the recovery component, technical assurance, risk management, I think are things that are kind of overlooked and not done as well as they can be most of the time. Given budgets, people gravitate towards you know, cyber defence, preventing bad stuff from happening in the first place. But you know, you could have numbers say if I've got good technical assurance, my incident numbers should go down because you know we're…we're doing a good job. So,  
by having less and less incidents, that's a really good key performance indicator that could be bought on through resolving the risk through good, good, good, good technical assurance, making sure we're turning on and using every bit of functionality. Yeah, so it's. Those are three key areas of thinker what we could.

**Interviewer** 35:18  
Mm hmm. Hmm. OK. And then so the question number 9 is, uh, what can you, what do you think can be helpful to make up such insufficient. Uh, such insufficiencies when you talk about it, technical assurance and risk management and recovery component. So how can you be helpful to make up such insufficiency.

**UPR3** 35:44  
Also, what can I do to make up for such inefficiencies?

**Interviewer** 35:47  
Yes, yes.

**UPR3** 35:49  
I think going back to where my department sits, if you sit in IT. If a security department sits in IT, what you will find is that you will generally have a good technical control environment. You probably won't have a very good technical assurance control environment. If you sit in a legal function, you will probably have a good risk management function and different strengths. It really depends on the department that you sit in, whether you're in technology or outside technology, about how things work. I personally don't think that information security should sit in IT. I think it should be an independent function that advises technology on what they should and shouldn't be doing, or to have a smaller team in there that that that does stuff. You know to do security well, it's people, processes, technology that are three core areas. If it sits in IT, as I said, technology is going to be strong. But…but for me it's about its people and processes that tends to get overlooked. Companies still think that cyber is just about protecting computers. It's not the impacts are a lot wider. The business impacts are a lot wider. So for me, I always try and make sure that when I…when I have a small team of people that I allocate them to all of the key areas that need to be done. But primarily you know the…the kind of the the people side of things. So yeah, the way to address the inefficiencies is…is, you know having a model that that kind of covers core security objectives and make sure you have adequate coverage because security is simple. It's about focus on core security objectives. You know, if it sits in IT, you have a poor focus on technology, but you won't have a core focus on people that know what they're doing when there's a cyberattack. You know, IT departments deal with IT incidents on a regular basis. The difference between a security incident and an IT incident is that behind a security incident, there is a human being with malicious intent. And IT incident. But they confuse the two. They think it's the same thing and it's like it's not. This is somebody who is really doing something. So sometimes removing security from IT is a better way of…of dealing with it and applying pressure on IT to do stuff in a particular way. If it's in house it's…it's all a bit blurred. It's a bit too confusing and what have you.

**Interviewer** 38:28  
So I can hear a lot of about you say the people is the key. Cause for the…the tech the technical aspect you can just use the IT the technical how do you say, to to improve but the human….

**UPR3** 38:48  
Yeah, I mean I…I…I could have just recruited one person that goes that sits kind of like very close to IT and provides a list of all of security that we've got, how good it is, how bad it is and then have an improvement plan in place. And that technology assurance piece you know can be…be done quite well. But it's a lot of it is understanding. You know, I've dealt with cyberattacks in other companies where I've been recruited. And the reason that the cyberattack failed is because the people didn't know what to do. They didn't know what it was and they didn't want to make a noise about it because they sat in IT and they didn't want to make a lot of noise. Now in security, you always err on the side of caution. You make a lot of noise about something that may be nothing because it doesn't matter. You know, who cares? You know whether you're right or wrong. But there is a…a mindset problem, I think, especially with security teams in IT. The, you know, that they also worry about the impact. Oh, well, I don't want to turn that computer off because that that user might get upset. And I'm like, excuse my French. I don't care about that user. I'd rather, my job is to protect the company. I'd rather disrupt one user and you know, be moaned at that. Oh my goodness. You know, you caused me a bit of bit of a problem. I don't, I don't care. But there is, there is people is a massive problem. You've got to have the right people, but with…with the right level of experience and what I always find, being an ex-police officer working in cybersecurity, is that a lot of the people who work in security are not curious. They're not inquisitive. They…they…they, they don't actually have the right skill set or the right mental skill set to do security because it takes, you know, a certain person. I I sometimes think if I had the choice, I would rather have somebody older, like, say, from a policing background who's curious, that will dig in that, you know, and have somebody younger as a technical person. And to help them work together. Because you know there's…there's…there's a gap where you need that, that curious, you know, kind of mindset and the understanding of the criminal mindset and the actors rear and the mentoring all of those are the bits that that go with it, that level of thinking and the technical know-how. But you can't find them both. They're generally two distinct, you know, kind of things. So actually having that older person, younger person, more tech savvy, having them working together, I think is a really good synergy to help bridge that kind of mind gap that I see quite a lot.

**Interviewer** 41:29   
Mm hmm mm hmm. OK. Thank you. So that you say that young the the young generation, they are more…the curiosity about the the cybersecurity, not the opposite.

**UPR3** 41:44  
No. Not necessarily, not necessarily younger generations, more people that sit in technology.

**Interviewer** 41:50  
OK, OK.

**UPR3** 41:52  
People that sit in technology, it's…it's a very black and white environment. Oh, the server's not working. Oh, because the power's gone off that, you know, they, they're their thought process is…is wrong and security tends to grow from an IT department. That's where it kind of it starts off and it's all about technical controls. But as…as you know. The company grows. There needs to be a shift in mindset and an IT person has a tendency not to have that. What they don't have an understanding of the threat, and that's what's missing. You know, they, they, they, they, they, they think they know. But you know what I found in the company I've worked before is that you know, I I've dealt with cybercriminals, Russian organised crime groups, malware, gangs, I've dealt with big cyberattacks, big ransomware attacks I've dealt with lots and lots of stuff, but then I go into an organisation and I…I inherit an IT department who does security stuff and I'm getting involved in some of the decision making processes. And they say no to things based on the most disproportionate level of risk. So I understand the threat better, you know. So I'll go. Yeah, go ahead and do that. Do it for two weeks. But no, don't go on for too long as my this is the department I've worked in. They're like, no, you can't do this. You can't this. You shouldn't do that. And then that starts to block the business. And and that's because they, you know, they're they're kind of their understanding of the threat is different because they don't know it. So they they're always err on the side of too much caution and think that everything's really bad when in reality it isn't that bad, you know. But, but yeah, there there is a a mindset. It's definitely a mindset, a mindset issue with, with, with security departments.

**Interviewer** 43:45  
Mm hmm. OK.  
Oh, and so let's go to question number 10. So in what aspect do you plan to improve the? Maybe the techniques or the services you provide? You know to for for the business or the general public or the yeah, private sectors or even the governmental organisations.

**UPR3** 44:16  
In my in my world, you know to get better is you know we use maturity assessments. So we'll get third party firm to come in and say, well, where do you think we are based on on what we have today and then use that as a benchmark to improve. You know every two years might get companies come in and and…and assess that. So you know for me security is quite simple. Focus on core security objectives and get better at it. And that's it. And have a way of measuring how you're getting better and then use an external company to…to help reinforce and assure and give confidence to the stakeholders or the shareholders that you know securities in a good place.

**Interviewer** 45:01  
Mm hmm. OK. Thank you. OK, so then let's go to Section G and Section G is about public private partnerships in terms of cybersecurity. So the question number one is I want to ask about your opinion on this partnerships. What do you think about this partnership? Does that really help in terms of cybersecurity?

**UPR3** 45:32  
on occasions. It may not often enough though.  
There is still a hesitance from the public sector to share information, but information that that makes a difference that we can actually do something with the information is always far too broad, far too general, and it's not enough to…to allow private companies to take, you know, action, you know against something and. Also, they're.  
Again, because cyber. There's it's quite narrow in their thinking. So let's say for example, you know a cyber attack that happened against the bank. You know, we may get some information from, you know, law enforcement, about a gang or…or something. But again, it's not detailed enough, but they're not. You know, they're not considering the fraud controls. They're not considering the anti-money laundering controls. They're not thinking about these wide and broad controls because an organisation has lots of different methods in place. They're not just technical in nature. You know, working with finance and making sure that they have a…a control in place to make sure high value transactions have a password or…or…or something is just as important control as a technical control. You know an anti-money laundering department that's…that's looking at suspicious activity and closing customer accounts down, based on, you know, information from a cyber group and what have you can just be as disruptive to the cyber gang from a from a money laundering perspective as well so. Yeah, I would say it helps, but it's not enough and it's generally too late. You know, every time I get an update from the FBI from GCHQ, it's probably three weeks after I already knew about it. Like, well, you know what? What's what's the value in that? Some companies will just wait for that, and that may be good enough. But you know, my team, we have a call every day of the week. We, you know, we find out this information because it's it's publicly available, you know, a new vulnerability, a critical vulnerability, an issue, whatever it is. So it's not enough and too late and the quality is poor and I can't see it increasing and getting better, you know, in time, because I think there is just this law enforcement slash, you know, confidentiality. They just need to get over it. They're not. They're not giving us names and details. It's specifics.

**Interviewer** 48:05  
Mm hmm.OK.

**UPR3** 48:11  
And…and a lot of a lot of the time law enforcement, you know, they're too slow. I mean, I've worked in it. I, you know, I…I used to think we did a great job. But I know that we're just too slow. You're too slow and you don't have minimal impact on..on…on…on cyber crime, global cyber crime.

**Interviewer** 48:30  
Mm hmm, I think that's a bureaucratic issue. They're always really slow, so I think you mentioned about the speed. The poor information quality and not enough information are the...

**UPR3** 48:46  
Yeah.

**Interviewer** 48:49  
Then number 2 question number 2 is as you know, do you know about any of the current public private partnerships mechanism?

**UPR3** 49:00  
Yeah, I think there's one SISP. Is it SISP? No, sis. Yes. Information sharing partnership. I think it's a GCHQ which is quite good. It's a good forum to get people around in the UK to share stuff that they're seeing. You know, again the problem with a lot of these forums is that most of the people that go to them are very junior people in an organisation. They don't really understand the world well enough. You know people, you know, like myself are kind of managers or a bit distant from it. So again, the kind of the quality of the sharing and the hesitance and and what have you know, is different. So it's…it's almost like. There needs to be more partnerships based on specific roles that you do, you know. So as head of information Security, I don't think there's you know there should be a kind of a proper government group that that provides input and allows me to engage with people at that level. You know there should be analysts who are doing daily work that engage a different level. So having a more at the moment, the SISP, the Information Security Partnership is just a…a group of people that all get together, that's industry specific. Everybody has completely different objectives and thoughts around what they want to do and what they want from it. You know, it's…it's, it's a bit of a mixed bag. So I think having that more role based intelligence sharing platform would be better.

**Interviewer** 50:30  
Mm. OK. And then what else can be improve in terms of the insufficiency you mentioned about?

**UPR3** 50:46  
From an intelligent sharing perspective or partnership perspective. Again, the problem is, is that law enforcement, quite rightly or GCHQ. They gravitate towards critical national infrastructure. You know, they gravitate towards high-risk infrastructure. You know they…they do that. So again, you're always going to have the gap around or what about all these other companies that are not critical national infrastructure, but bring an awful lot of money into the UK and are not getting the same value that they're getting because they don't fit the definition. It's almost like, you know, you need to. I don't know. Was so if security's simple, right? Sometimes you know if. If you're if you're. If you live in a house. It's got lots of big lights on and got guard dogs outside and and…and then you got a house next door that's got no…no guard dogs. That's got no lights and you're a burglar, which…which, which one do you attack? Which one would you try and steal from? The ones with no security controls in place. Right? So that's what's happened is that indirectly, countries are creating, you know, they're creating the new targets because they're saying to one section of the business, you need to become really strong and hard here. And they don't talk about everyone else. So it needs to be looked at.

**Interviewer** 51:53  
Mm hmm.

**UPR3** 52:08  
You know, if you're doing a security strategy on Taiwan and you know you're looking at your different sectors, you put them all up into different sectors and you know you consider more, you don't just consider critical national infrastructure, but be you also consider, you know, GDP, you know the value that this company also brings in place. So the criteria around what we need to protect needs to be a bit broader and not just critical national infrastructure.

**Interviewer** 52:25  
Mm hmm. Mm hmm.

**UPR3** 52:37  
That don’t get me wrong. It's important. It's. But it's about striking the right balance because now what you have in the US and the UK and a lot of Western society is, you know, stronger critical national infrastructure, you know, environments. But the rest of the country is getting ripped apart through ransomware, fraud and all these other attacks because they don't have the controls in place because, you know, we forgot, not we forgot. It's there needs to be a…a…a standard mechanism, or a control piece. And I tell one of the biggest issues with the whole cybersecurity world is third parties. Honestly, that is that if that is the worst thing ever. Because…No. Tell me what you can do so you pay electric, gas, rent, broadband bills at home, right. Yeah. What influence can you have on…on the security of the departments that provide you with those services? What impact can you have? What can you have? No impact, right?

**Interviewer** 53:52  
Mm hmm.

**UPR3** 53:53  
But this but this is what you know. So let's say for example a bank may have may have 10,000 third parties. They will recruit a whole team of people to manage third parties to make sure that they have the appropriate controls in place to reduce risks, to reduce their supply chain risk. Now those third parties of 10,000 are a customer of bank one bank, two bank, three, bank four, bank five and they're all being asked exactly the same questions every single day. Multiply that by 1000.

**Interviewer** 54:10  
Mm hmm.  
Mm.

**UPR3** 54:25  
Now those companies. And now not spending their time on security, they're spending the time filling in questionnaires to banks or somebody else. And it's almost like this third party risk management piece is…is ridiculous and I it's such an inhibitor to growth, you know, because you have all of these third party companies that they, they recruit people just to deal with third party risk. And but the point is…is that what influence do you really have on another company? No. You can't do anything, so third party risk management which is seen as a big control, is the messiest area ever. And you know it's almost like, I would, as a government, I would set up a department, call it third party risk management or something and offer a certification programme that, you know, if I'm an IT supplier, I get a, you know, I'm assured by and I don't have to fill in a questionnaire. I don't have to. You know, I don't have to do it 10,000 times. Because that's actually making the world less secure. Because if you have one company that's focusing on, you know, all their time and effort and money and budget on managing questions from banks times 1000, they're not spending the time on security. So that actually is having a negative impact on security and it's…it's something I think that needs to be resolved because it is, it is, it's the most ridiculous thing ever. And but everybody wants to do it. But most of the time, the only reason they do it is that when it goes wrong, they can turn around and say, but look at what I've been doing. But it's you have no effect, you can't affect it, you know, unless you're going to go around an audit, every single company. You know it's…it's an absolute madhouse. And, you know, multiply that by third. It's happening all over the world, right? But if there was just a standard, you know I'm third party. I go to one company, I get credited by government department, which means leave me alone. I've done enough. And I've done enough, you know? And it just because people need somebody to blame when it goes wrong.  
That's what happens. But if there's a government there that says that we've confirmed and endorsed it, the government can withstand that kind of that, that kind of backlash, you know.

**Interviewer** 56:47  
Mm hmm.

**UPR3** 56:51  
But yeah, so yeah, third party risk might got, get on top of that. That that would make a significant…really good plan on how to manage that 'cause it just means that everyone in Taiwan, if that programme was in place, they can just focus on security of their own company, not getting lost in questionnaires for other banks and everyone else multiplied by 1000. So I think it's just it's an efficiency ruling.

**Interviewer** 57:07  
OK.

**UPR3** 57:17  
Just to take away from me, it's one of my frustrations everywhere I go.

**Interviewer** 57:22  
OK. So third parties risk. Yeah, quite interesting angle, yeah.

**UPR3** 57:28  
Because because that because because. Because that goes back to the point I'm talking about the reason that third party risk is so big is because banks and critical national infrastructure have been regulated for so long that the threat is now manifesting in less controlled environments. That's where why we have what we have. That's now why banks are going around trying to manage third party risk, but they're causing more problems than needed. No, it should be one questionnaire to one company. Not every single bank that asks the same question in a different way, you know multiplied by 10,000 different customers. It's like and these people are just sitting there. These companies going, they're just thinking, you know going how can I do this, you know? And spending time and effort on doing it. Just one question you know.

**Interviewer** 58:02  
Mm. Mm hmm.

**UPR3** 58:17  
And the problem is…is that different companies will have different risk appetites, right? Bank. You know, they've got a hybrid, you know, very low tolerance for risk. You know, other organisations may have a higher tolerance and the questions are different and it's…it's painful for them because I've…I've sat as a third party and I've, I've done both sides of it, but anyway.

**Interviewer** 58:23  
Mm hmm. Mm hmm mm hmm.  
OK. So like you said, every…every bank. So every third party they have different kind of cybersecurity risks, so you have to tailor down the like. Maybe specific, not just questionnaire, maybe some strategies for them to deal with, not just every bank. You. You give them the same question every day and they just spend all…all the time to fill out these forms and questionnaire. Is what you mean, right?

**UPR3** 59:12  
Oh yeah, because every bank has a third-party risk management department. I'm. I'm. I'm using banks as an example. You know, a…a technology provider may have 100,000 different customers. You know, out of those customers, you know, 20% of them could be banks, 20% of them could be, you know, oil and gas. So they've still got the same problems, but all of those different companies are all asking the same questions. You know, it's almost like there needs to be maybe a…It just needs to be simplified. Because it is, it is drowning these companies that they need to spend more time and effort on protecting their organisations are getting lost in asking questionnaires and dealing with third party risk departments. It's like there just needs to be something that says stop. I've got this accreditation from the government that says I'm good enough to be on your supplier list, you know, and that's it, you know? And governments say, yeah, that's good enough. They passed this standard. You know, maybe the company has to spend a bit of money on an audit or something.  
Ummm but you know, some companies, whether you're ISO 27,001 whether you're SOC 2, whether you're this. Every company will have a different requirement. And well, that's not good enough. We need you to have this. It's just like. Anyway. Difficult.

**Interviewer** 1:00:34  
OK then I want to ask you about, you know, for the future public private partnerships, what do you think that maybe the public sector can contribute and also the private sectors can contribute to make this cooperation works better in the future?

**UPR3** 1:00:59  
Yeah, maybe have more, more kind of joint. Umm, when…when I was in the police. My understanding of the threat to an organisation was completely different to when I was in the private sector. I didn't understand it, so I think better collaboration from a like almost work placement. You know get people, you know who are in law enforcement and vice versa, you know to and maybe not the other way round as much because it's more important than law enforcement understand how businesses operate and that they understand what the risks are and the challenges that they pose. But they don't. They don't understand it well enough. So therefore the material and what they produce doesn't hit the mark, you know quite well enough, to maybe kind of some kind of, you know, more partnerships around work placement schemes for law enforcement. I mean I…I…I when I was in the police, I left the police but I still stayed on as a police special. And what I was doing was working with the police, understanding some of the cases that they had. I would then write an Intelligence report that would land with the company that I worked in that would hit. This is what the fraud team needs to do. This is what the cyber team needs to do. This is what the money laundering team needs to consider and then produce that as an Intelligence report which meant that that landed an awful lot better. So it is…it's…it's law enforcement, don't understand business well enough as I didn't. They think they do.  
But they don't understand the challenges, you know, w ell enough, you know, especially when it comes to money and budgets and you know in the police you don't think about money. You don't. You know, you generally just you know it's…it's there you know the your bosses may think about money but most police officers don't.

**Interviewer** 1:02:45  
Mm hmm.

**UPR3** 1:02:54  
So.

**Interviewer** 1:02:57  
OK, so that's why they.

**UPR3** 1:02:57  
Yeah. So. Yeah, so better…better closer partnerships I think.

**Interviewer** 1:03:02  
Mm hmm. Then then what do you think the law enforcement can contribute to these partnerships that they need the private sectors to to cover up the the? Now you know that because you said you they don't understand about businesses. So that's why they need private sector to come in to help them with this area. But then what can they contribute? What can a law enforcement contribute to the partnerships?

**UPR3** 1:03:36  
I guess it's more…more timely. Relevant information. That's hot off the press, not too late. You know, I think I think law enforcement. You know, can there's a very well, it's like if you were thinking law enforcement predict prevent, detect, respond, recover. You know I would expect law enforcement to be providing good intelligence under the predict strand. I would expect them to be providing good preventative information and and…and structures predict prevent detect. Maybe to help with detect? On the response piece that they can help, but most crime that we deal with is global in nature. So it's very difficult for one law enforcement to deal with it and even when they do deal with it, the impact is…is short lived. So it's almost like looking across, you know, the police or law enforcement strategy and setting down. But what are the products and services that we can provide to the private sector based on our strategy? Because they're looking at securing the country, but they secure the country by making sure that we…we have better controls in place, right, the government department. So it's…it's almost like you know, again law enforcement like to come up with their own security models, you know, because they don't use what everyone else is using use nest, use ISO, whatever it is you know use predict, prevent, detect, respond or…or…or whatever the NIST standard is you know.

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

**UPR3** 1:05:17  
And you know, just use that the communication and the way in which they structure stuff is different. But, you know, I think we all, we all need to align on a common language of security. And especially when it comes to a framework, because you know an American company, it's in the UK or, you know, everyone will be doing something different. And I think this new act that's coming out, Dora. The digital Operational Resilience Act, have you heard of that one? So to say Dora is is probably a good step in the right direction because it's about an EU framework to increase cyber resilience. So cybersecurity is an old world word, you know, even information security is becoming an old world. It's all about resilience. It's about, you know, we are all operating in the cyber domain. How do we as an organisation make sure that we're hardened, you know, to think so this new act is a European piece.

**Interviewer** 1:05:57  
Mm hmm. Mm hmm mm. Mm hmm.

**UPR3** 1:06:18  
So maybe that will help. Kind of create a language to speak on, and Dora again is aimed at critical national infrastructure. It's aimed at finance. But it should be broader than that. It should be. You know, the banks need to be doing this at 100%. These sectors need to be doing it at 75%. These organisations need to at least achieve 50% or whatever it is, but it's never landed like that. It's like it's just for banks, you know. I think it is quite rightly because you know as a as a country, you know we want to protect our digital borders, right. And so I get why we go, we go down the critical national infrastructure route. It's just recognising the fact that by doing so you create a disproportionate level of risk elsewhere. So what is the strategy in place, you know to…to kind of to mitigate that?

**Interviewer** 1:06:55  
OK, so you said Dora's Dora is a….

**UPR3** 1:07:15  
Yeah, yeah. Digital Operational Resilience Act.

**Interviewer** 1:07:18  
OK, I will have a look after this so.

**UPR3** 1:07:22  
Yeah, that's that's EU stuff, you know.

**Interviewer** 1:07:25  
OK, EU stuff.

**UPR3** 1:07:27  
What I see a lot of the time is, is that the world and you know you, you may see this, you do, you're doing criminology. But. What I think's happening is. Countries are emulating their physical borders, and they're creating the same in the cyber domain. So how how? How does a country protect its digital borders. It does it by introducing legislation and regulation to stop you from. You can't do this. You can't do that. So I think you know probably 20-30 years down the road, maybe sooner you know we are seeing. You know. I just see this whole freedom of movement within the EU. You know, we can see it, you know, in China and the US and the Great Wall firewall of China and stuff that what we're seeing is, you know, the geographical borders that we have being emulated in the, in the cyber domain. And that's happening through through, through, through regulation and stuff. So it's…it's interesting, you know, the way in which the world's…world's shifting.

**Interviewer** 1:08:28  
Yeah. Yeah, it is. OK, so I'll have the last question for you. So can you tell me about your experience on the private public private partnerships, if you have, you know any of the?

**UPR3** 1:08:51  
Yeah, I well, I used to be in one. I can't remember what it was called.  
Because I was in the police engineer crime unit. So that was the first department in England to be set up to tackle cyber crime. And again, that was a private partnership between the police and banks, and that was quite good because we were trying to get a better understanding of cyber crime and how to detect and respond to it because we didn't know, you know, police didn't know. We know it's we didn't know what was going on. So the that worked really well. Is that the banks providing us with…with good insight into…Into different…different attacks that they were suffering from and the cases that we dealt with there. I dealt with one about Russian organised crime groups and actually how it linked into a changing political situation in another country. So it's quite interesting how a political climate in one country actually led to an increase in cyber crime in, in, in the UK and…and globally and that…that partnership was really good at to begin with. It's just maintaining the momentum.  
And I think. You know, I think it's a better working relationships as well between GCHQ, law enforcement. So you're kind of more intelligent services working better with law enforcement and the and the and the private sector. And you know, coming up with, you know, strategies that, you know, the intelligence community is going to do, this law enforcement are going to do this. You know, we are all gonna do this.

**Interviewer** 1:10:31  
Hmm.

**UPR3** 1:10:33  
But again, thinking a bit wider, you know people think cybercrime. They think technology. It's not, it's it's…it's technical controls. It's as I said, anti-money laundering controls it's there's lots of other ways to, to, to, to kind of disrupt criminality, but it's about being joined up and coming up with different strategies that you can all execute, you know, to, to, to kind of to mitigate a particular threat.

**Interviewer** 1:10:52  
OK. It's interesting and, but have you ever encountered any difficulties during these partnerships?

**UPR3** 1:11:15  
Yeah, I think that the problem I've found is that when I worked in banks, for example.  
I had very strong intelligence working relationships because the law enforcement wanted to know me. Because I had access to banking data, I'd access to things. Now I leave that sector nobody wanted to know me. Sources is again, it's all geared up towards critical national infrastructure. It's not, I mean the demand probably isn't there as much sometimes in, in other sectors. I move from banking into…into tobacco for example. You know I didn't have bank account details. You know, I had nothing that was of interest. So my U.S. law enforcement contacts dried up and disappeared. My, my, my UK sources disappeared. It's because they're all focused on one sector. So yeah, that was new. And so I kind of lost touch with them, but it was it was, you know, when I worked in those sectors, it was very strong.

**Interviewer** 1:12:19  
And then what do you think can be improved  
You know 'cause you you said you are. You just mentioned difficulties that you encounter then maybe you lost the links with them or things like that and then then.  
How can the improve if I I know you have. You have left the the unit but how can be improved if you're still working or…for them. With them, yeah.

**UPR3** 1:12:58  
Yeah, I guess it's. I think it's been out…out more. I…I…I…I think that that the law enforcement can probably do a a better job of awareness. You know, if I had, you know, if I had a daily call which I have every day and if I could get somebody from the police to join my daily call for 15 minutes and just take them through a cyberattack, they they've been dealing with. You know that would help bring it to life better, you know? So I…I actually think on the awareness front, you know, get out there, talk about what's going on, let people know what's going on, you know, join.  
Companies daily calls, you know, do a 15 minute presentation here. Just get stuck in.  
You know, just get…get the message out there better. And you know, help bring it to life, you know, and, you know, law enforcement in a private company has a big impact. You know me telling them when I was ex law enforcement is all right, but doesn't have as bigger impacts as somebody that's actually in the police doing it now. So I think they can play a far stronger part on, on, on, on awareness and helping drive that message home to every sector. And stop just focusing just on critical national infrastructure.

**Interviewer** 1:14:11  
OK, so awareness and help to transfer this messages out to the general public.

**UPR3** 1:14:27  
Yeah, yeah, yeah.

**Interviewer** 1:14:28  
Yeah. Yeah. OK. So yeah, I think that's it. Yeah, I think I got a lot of information. So let me just, just press stop.