This document contains the full quote and leading question(s) for the quote where appropriate. Where interviews were not recorded, then the relevant used notes have been provided.

Questions or context are put in square brackets and new content which was not used in the original thesis has been highlighted in grey.

See DOI (Thesis): 10.5258/SOTON/T0036 for more information.

For participant information, please see the participant table.

Awareness and cost of PBX Hacking, Toll Fraud and IRSF

Overall Lack of Awareness

**Policy Specialists & NRA**

[Were you aware of PBX Fraud?]

*“specific form of cybercrime with a large entry point.”* (P14)

[So PBX fraud is an enabler?]

*“Exactly, because, you can call multiple numbers”*. (P6)

[So a missed call from a number?]

*“Yes, but I wasn’t aware of this specific use case of criminals hacking PBXs” (P7)*

*“I have heard about people getting tricked into calling exuberant destinations” (P7)*

[Were you aware of PBX Fraud?]

*“I wasn’t aware that it was called PBX Fraud for instance, but I was aware of hacking into telephone systems to conduct Toll Fraud”. (P5)*

[Are you aware of PBX (Company Phone System) hacking (commonly known as Toll Fraud) and the suspected global cost per year? If so, please tell me what you know.]

*“We are aware of this type of fraud but do not have any further information such as on the frequency of its occurrence and/or the resulting financial impact.”* (P4)

[Based on my stakeholder experience and research, are you aware that some hacked PBX calls are calling other countries inside the EU which do not follow the lower landline or mobile termination rate costing model?]

*“We have not received any specific reports of such cases.”* (P4)

[Explained provisional findings of Honeypot]

*“Is the vulnerability a network vulnerability or device vulnerability? Basically, do you hack into the end point. So it is not an issue with the network operator?”* (P5)

[The attackers target the PBX and the numbers they call, they usually have a financial interest in. So they get a rebate every time a call is put onto that number]

*“Is he a knowing participant?”* (P6)

*“Is the receiver of the call in on it?”* (P7)

[No Question – general discussion and point made]

*“Interested to find out more such as how it works*” (P13)

**Lawyers**

[Are you aware PBX hacking, Toll Fraud and the suspected cost around that?]

*“I’m familiar with various attacks against telecom companies and various exploits depriving them of revenue or taking revenue that shouldn’t otherwise be acquired” (P18)*

[I am investigating PBX hacking, Toll Traud etc. End users when their business equipment has been compromised.]

*“So this is the scenario when a user has deployed some form of equipment within the premises and someone compromises say their VoIP credentials” (P18)*

[Yes, so for example, a company sets up their own PBX system and through their incorrect configuration of it.]

*“So getting into their PBX and making calls through there PBX” (P18)*

[In some respects, it’s the perfect crime? (After P17 Comment: *“No wonder, it is so easy todo”)]*

*“It is the perfect crime. On top of that, you do not have a specific victim except the company which is ultimate due to pay you money, but then this company can tell we have a contract and we are just executing the contract. Where this is no actual phone calls.” (P17)*

[Were you aware that some of these calls go to European countries?]

*“No, how is that possible?”* (P17)

**Cyber Security Specialists**

[Prior to our conversation, were you aware that PBXs were being hacked to make calls that would essentially cost businesses money, in some cases, significant amounts?]

*“Yes [Aware of PBX hacking], but not for this, I have been tracking an APT group who hacked different phone networks to track individuals, but I was not aware of this scam.” (P2)*

*[Are you aware of PBX hacking, where for example a phone system could be hacked and could run up a large phone bill where money is in effect stolen from that organisation?]*

*“So, I think the potential of it being a threat was something I was aware of, but in terms of it being so imminent was not at the top of my threat analysis, but based on what you have informed me, it is clear that this a growing area and specifically given the way industry standards are going towards voice over IP, we are starting to see now that mobile phones are having the option of accepting calls.” (P1)* (Accepting calls in reference to Unified Communications)

[Prior to us discussing, were you aware of phone systems being hacked which caused large phone bills for companies?]

*“No, but I’m aware of when you receive a phone call and they expect you to call back and I guess they receive some payment for doing so.” (P3)*

**IT Director & Trust Expert**

The TPE was not aware of PBX hacking specifically, but was aware of other telecom frauds:

[Building off when you said you were aware, could you expand? providing any examples and how long ago was this?]

*“I was aware of a lot of scams going on the telephone. Two types primarily. One trying to get you to interact with premium numbers without you actually knowing.” (P20)*

*[Are you referring to receiving a missed call and you calling that number back thinking it is a genuine number. For example, an 070 number, you may think this is a mobile because it begins with 07, but actually you could call it a premium rate because of the excessive charge?]*

Where the TPE confirmed on follow up that they were referring to missed call fraud. While TPE explains the other fraud being:

*“The other is when you receive a call which says we’ve noticed you have a problem with your computer” (P20)*

When asking ITD if they knew what Toll Fraud was, their response was:

*[Are you familiar with what Toll Fraud is?]*

*“Would that be when people are spoofing numbers or they call in and they dial back and you look like your dialling toll free but it’s a chargeable number?” (P16)*

[Not quite. Simply you have your corporate phone system and a third party attacker breaks into your phone system and uses your phone system as a gateway to make calls to numbers they have some form of interest in.]

*“Oh right. Yes I know what you mean. We’ve had this.” (P16)*

[What was the region of spend?]

*“It was in the thousands.”* (P16)

[Was it low or high thousands?]

*“I can’t remember, but we’ve had a number of breaches. We’ve moved to Exchange online, we’ve moved to 365 and that in itself brings its own challenges. We have MFA on a lot of users, not everyone. This is on Skype for business for example. So if you’re in a country where Microsoft has infrastructure, UK, USA, France for example, you could buy a calling licence. For most countries, they do not have that in place. For example, if you want to run Skype for business in Russia, you must have a Session Border Controller, you take a SIP trunk into the Session Border Controller, preferably 2 of them so you have failover. Skype then connects to the SBC for external calls.”* (P16)

*“So in our instance, what happened was that someone hacked someone’s account, they gone into office, installed Skype.”* (P16)

[Ok, this is new as I’ve only ever come across this on the SIP and PBX side, I have not come across a corporate hacked office account before.]

*“So, they’ve done it into Skype and set the dialler up. Normally our provider is hot on blocking them, which for us can be problematic as we call frequently many of these countries regularly. What I recall was a high volume of calls to those particular numbers and I recall the cost being in the low thousands for that one user. We reset our passwords regularly, we insist on complex passwords. So, we have restricted that to an extent.”* (P16)

[Going back to that account that was compromised that spent several thousand pounds. Over what time duration was that?]

*“It was picked up after about 4 days. We’ve got a call reporting system which goes out every 24 hours so it was only because no one had looked at it and when we did we thought wow wow wow. This person has just made 2,000 calls today, we went over to them asking have you made any calls today and they said no.”* (P16)

Unaware of the cost

[How much do you think this costs globally each year?]

*“Millions?” (P16)*

[Do you have any idea how much this is likely to cost globaly per year?]

*“Many millions, but I do not know.” (P2)*

[What are your thoughts on those figures and the costs?]

*“It’s surprisingly low, I would have expected a lot more…”* (P20)

*“…if I look at the cybercrime and compare this to others of the things I look at, such as fake news where there has been a lot of allegations since 2016 of bots and their role with foreign agents,* *specifically the Russians being blamed as a major source of inappropriate material on the internet, given that background, if it was relatively easy todo, the financial implications would be much higher”* (P20)

[In terms of the suspected cost of PBX hacking, do you have any idea of what the cost is per year globally?]

*“…I think in this type of fraud it is easy to put a dollar figure because you know how much it is costing for each minute, which is rare in Cyber Security.” (P3)*

How hackers financially benefit

[Have they heard of this fraud and aware of the costs?]

*“The participant had not heard of this kind of fraud and was interested to find out more such as how it works.” (P13)*

*[I am investigating PBX hacking, where phone systems are being hacked and attacked, where hackers are calling numbers all over the world that generate a revenue. If you read industry reports, we are discussing figures that are in the billions, if not tens of billions depending on the source of your figures.]*

*“How are the hackers being able to make money as they are just hacking in?” (P17)*

*[Yes, there are some EU terminated calls, but generally its calling outside. The number ranges they call are premium rate defined numbers which from an operator is very easy to block, but some times they are geographical or mobile ranges.]*

*“How does the fraudster make the money?” (P5)*

*[It can actually be a geographic number.]*

*“So, do they make the money?” (P5)*

*[Explained Honeypot experiment]*

*“So how do they make their money?” (P6)*

[So, in the case of PBX hacking, where they are calling destination that are fairly expensive, were you aware they were calling regular landline and mobile numbers?]

*“So, I think there are a number of different channels for it, because simply calling numbers that are expensive doesn’t result in any particular gain to the organisation that has compromised the PBX and if they need to make money then they somehow need to be in the supply chain”* (P18)

[Essentially, they are trying to get free traffic for their customers?]

*“Exactly, or the other situation where they are also the other side of the traffic where they are somehow in the supply chain where they are benefiting from withholding some of the money before passing remainder on to whoever is downstream of them.”* (P18)

*“Yes, and if for example you were looking to setup a calling card business where I handout a card with an access number on it, you dial the access number, you think you’re dialling into the providers network, but really you’re just routing the call through the compromised PBX. The numbering is in effect irrelevant and the cost saving to the hacker is that they don’t have any transit charges. Yes, it makes sense to me that we are not necessarily talking about where the recipient is a premium rate service operator which is retaining revenue at the end of it. It could be at the beginning taking money directly from someone’s hand in exchange for a calling card and have a low or zero cost of supply by not having to account for the transit.”* (P18)

Failure to understand geographic numbers

[Aware calls can be to geographic numbers?]

*“Participant did not know non-geographic numbers, let alone geographic numbers could be used like this, although understood how it worked” (P17) (notes from follow up with participant)*

*“had a hard time in understanding that calls were not necessarily to non-geographic numbers” (P10)*

*[Yes, there are some EU terminated calls, but generally its calling outside. The number ranges they call are premium rate defined numbers which from an operator is very easy to block, but some times they are geographical or mobile ranges.]*

*“So how do they make the money?” (P5)*

Who is doing this?

[Building off that, depending on the source. Some say approx. 8 billion USD globally, others over 1 billion GBP in the UK alone. Because of the amount of money involved in Telephony Fraud, the complexities of the telephony markets and the nicheness of the skill set areas that this is required to do this, especially in moving the money around, who do you think could be doing this?]

*“Lets be clear. If this was one person in his bedroom he would be found out because of all that money.” (P17)*

*“At the end of the day, this is hand in hand with money laundering and you cannot launder without raising questions and being noticed.” (P17)*

*“So certainly, something to do with the power or administration in place” (P17)*

*“It could be at local level, federal level. We do not know. But I cannot believe and if we take the lower of the amounts, surely to be able to pass it through tax authorities, how do you do that? When the fraud is that big, this is when it should raise concern because obviously something has gone wrong.” (P17)*

[Would you say this is an APT or behaviour of an APT?]

*“Yes, I think so” (P1)*

[Prior to our conversation, were you aware that PBXs were being hacked to make calls that would essentially cost businesses money, in some cases significant amounts?]

*“Yes, but not for this, I have been tracking an APT group who hacked different phone networks to track individuals, but I was not aware of this scam”* (P2)

[Are you familiar with the countries they call.]

*“Yes, all over. We got hit from China, Russia, for example. These are the countries we most see. I think we also had Malaysia” (P16)*

[If I gave some examples, were they African, remote locations for examples?]

*“I remember some were to African countries, but can’t remember which ones. I was notified because we had some very weird large billing, automatic diallers pinging out to these numbers which we now get alerts on.” (P16)*

[Possibly, but we do not really know. – Response to P17 suggesting they would not be amazed if attacks originated from Russia.]

*“Have you seen the map of all the hacks that have happened over the past 10 years? That has been released by the US Department. It is very interesting as they have put red dots of all IT hackings and you can see the US, North America is particularly exposed and you also see that Europe is particularly exposed and it is very interesting to see how little Russia is exposed…” (P17)*

*“…you see little red dots all over Europe, all over North America and you barely have any in Russia, it is odd.” (P17)*

*“It would not surprise me if you said to me that a lot of the hackers are based in Russia”* (P17)

[So they have numbers registered in other countries, they hack the PBX because of some vulnerability. They then get the PBX to make the calls to those numbers. Does that make sense?]

*“Yes, so they are located in a country which has a dodgy service provider, maybe somewhere like Russia somewhere where there is no recourse to tracing them” (P2)*

[Essentially, they are trying to get free traffic for their customers?]

*“Exactly, or the other situation where they are also the other side of the traffic where they are somehow in the supply chain where they are benefiting from withholding some of the money before passing remainder on to whoever is downstream of them.” (P18)*

Payment Services Sector Comparison

Fraud, Terrorism Funding and Money Laundering

[Al-Quadia, Mumbai bombings, the FBI were able to link several million USD went from this kind of fraud to them. They did not claim money went specifically to that attack, but went to the organisation that arranged it. I try not to make this about terrorism, but there is evidence to suggest it]

*“It funds organised crime, which goes onto fund terrorism.”* (P5)

[Can you understand how this can be a risk to businesses for example from a financial, bankruptcy risk, terrorism funding, reputation.]

*“Yes. Fraud is always a risk to business”* (P5)

[Been linked to funding terrorism, FBI have linked the Mumbai bombings.]

*“No wonder, it is so easy to do”* (P17)

[Kind of, but they do post checks usually once some kind of damage has been done.]

*“So the phone calls have been made, money has gone to this account. Is the money then actually paid out to an actual bank account in that country?”* (P2)

*[These are just regular landline numbers – showing Honeypot results]*

*“I would be interested in seeing what is happening on the bank side. Because obviously whoever is doing this obviously is not present in all those countries. KYC is a big thing these days.”* (P2)

*[In this part of the world.]*

*“True. If they can find a service somewhere that allows the remote opening of accounts, then yea.”* (P2)

[So, the FBI have linked this to funding terrorist organisations. Such as that behind the Mumbai bombings of 2008.]

[So, to summarise, you had very little awareness and had no real idea of what the cost was?]

*“Wow… …No I didn’t”* (P2)

[Were you aware next generation electronic communication networks, such as voip could be used as a mechanism to steal this volume of money? Such as facilitate money laundering.]

*“I think the key word there is facilitate and therefore yes”* (P3)

[Can you understand how this can be a risk to business, not just from getting hacked, but by being presented with a large bill afterwards, especially if they are a small business which could put that business out of business.]

*“This type of attack will only harm the financial assets of the company. I don’t think it would do any type of brand damage or reputation to the business*.” (P3)

[I’m referring to specifically small businesses.]

*“Still so, but it will also affect their financial and maybe their survival too. To clarify what I mean is in a cyber-attack, the financial status of the company is not always the objective of the attack, sometimes the objective is not to cause them financial loss, but to cause them to lose reputation.”* (P3)

[Yes, the international access onto the range is most likely higher than that from a domestic call. So a lot of calls can go to remote islands, African countries, special rural areas such as that in South America, in the amazon for instance.]

*“So the terminating operator is complicit in the fraud?”* (P5)

[There would have to be an agreement somewhere, but realistically they are directly or indirectly involved because they are facilitating the call at the end of the day. It switching onto their ranges and some of the operators in the supply chain are big names, so it is doubtful they know about it.]

*“Is it common? That an operator has an agreement with a private company or even private person? To pay out revenue from the termination rate?”* (P5)

Comparisons between financial and telecom sectors

[So, if we compare this to credit card fraud, this are similar amounts of money involved and think how much is being done to combat that type of fraud.]

*“There is probably a far less investment gone into this. There is a lot of money put into preventing credit card fraud because the bank needs to indemnify the customer. However, with a PBX or phone system?”* (P16)

[More good will?]

*“Yes. I assume, that in a B2B setting they may also offer advice, anti-fraud services or something, not for free, not because they are legally obliged to, but because they see a business case in the package. Oh and by the way, we can help you avoid these issues, without taking any responsibility whatsoever”* (P7)

[An advisory service?]

*“Yes, just like you get a bank loan and they offer you a life insurance policy.”* (P7)

[So, building off what you are saying, are you saying the responsibility should be shared based on the size of the customer? I.e. what is the size and technical capability of the customer?]

*“I was thinking about the payments industry”* (P17)

*“…I think a comparison with the payments system is a good one. Especially as PSD2 Directive is going to be released.”* (P17)

*“...why couldn’t we put certain responsibilities on each stakeholder on the whole chain?”* (P17)

*“that is what we are doing with the payments system, companies issuing cards, companies running the payments systems and the customers all have certain responsibilities”* (P17)

*“The customers who are also the consumers have responsibilities, the shops allow payments have certain responsibilities, it is a complex system. But each actor along the line of the payment has certain responsibilities and this seems to me that this vision is lacking in this case and perhaps the European legislator will find a way through that.”* (P17)

Responsibility and Mitigations

Shared Responsibility

**Responsibility based on how much control**

[As these attacks are highly sophisticated, do you think it is fair for the responsibility to be on the customers end in defending themselves against this?]

*“I don’t see it as being a functional possibility for the service provider to take liability. Because if it is this large-scale thing, then in the first instance it is not something the service provider physically controls then it has to be the person who is physically in charge of the PBX system, the person who actually maintains it should be the one tasked with securing it. If you’re renting your system, that is a different kettle of fish.”* (P2)

[If we look at a cloud provider doing this, where you are arguably renting a partition, it comes down to how much control you have over configurability.]

*“Yes”* (P2)

*“It is on a spectrum between who is responsible, and devil is in the detail”* (P18)

*“Depends how much control there is depends on how much responsibility they should be given. (for example, if they have lots of configuration control, then they should have more responsibility)”* (P18)

[Would you say a collaborative approach, i.e. multiple stakeholders?]

*“Yes, which is better than deciding whether a specific or threat actor should have a duty to inform as that is a different question.”* (P19)

[So, do you think an operator has a duty of care to their customer?]

*“Yes. However, it depends who is best placed to do something about it. Does the provider have the means though?”* (P19)

[As this is arguably affecting more small businesses possibly due to less resources, where do you think the responsibility should be? Should this be more on the operator to inform their customer or should the customer be taking their own responsibility?]

*“who from the operators perspective is best positioned to spot that type of fraud*” (P17)

*“So even if the end customer is NEC and is a professional in the sector, lets say they do not have the technical means to check on the lines precisely what’s going on other than protecting themselves by firewall or other means, maybe we should look into spreading that burden in order to make sure the provider that can check on its line should be able to at least alert the customer. Responsibility in this case is the more important point, but as with anything in technology it is a mix between technology and policy.”* (P17)

*“you have to distinguish between professionals who should be aware and professionals who have the technical means to prevent it”* (P17)

*“So there were things that cannot be done unless you have the technological ability to do something and there are things you will have to do because regulators tell you to do.”* (P17)

**CP monitoring and providing tools**

[So, if I am understanding correctly if you have an organisation who installs their own phone system where they have complete control over it. Then do you think in the supply chain there should be some protections in place?]

*“So it should be really easy for the service provider to see a massive difference in normal use. At the very least you should be able to block that for a second and confirm”* (P2)

[Do you think businesses should be made aware specifically of this kind of risk by their provider and if so, how?]

*“The provider should be aware of this risk, the business goes to the provider to obtain the service. In terms of the business being aware of it, I believe in my opinion the provider should already have controls in place to reduce the risk of this occurring. Because of how the attacks occur being on the customers equipment though I can see that technically this would not be the providers direct responsibility”* (P1)

[Building and summarising your point, your suggesting the service providers should really provide them with the means to assist in helping themselves?]

*“That is correct. They give them the tools to protect themselves”* (P3)

*“There should be more monitoring to prevent escalation*” (P17) *(notes from follow up with participant)*

**Each stakeholder has a part to play**

[Building off that, where do you think responsibility should be? Should the customer be responsible themselves or should for example the network operator how more of a duty of care towards them?]

*“I think generally with this kind of risk it is a shared responsibility. But also from the public side, from the operator side, from the end user side and I don’t think you should only identify one party.”* (P5)

*“…it is shared responsibility, you need to have the operator provide the network, make their customers aware of it. You have to have regulators or public authorities making people aware.”* (P5)

*“Believed that responsibility should be shared”* (P17) *(notes from follow up with participant)*

[So, building off what you are saying, are you saying the responsibility should be shared based on the size of the customer? i.e what is the size and technical capability of the customer?]

*“...why couldn’t we put certain responsibilities on each stakeholder on the whole chain?”* (P17)

[As this is arguably affecting more small businesses possibly due to less resources, where do you think the responsibility should be? Should this be more on the operator to inform their customer or should the customer be taking their own reasonability?]

*“interesting because it crosses different areas.”* (P17)

*“…depends who your customer is.”* (P17)

*“…NEC and KPN case law is a good example”* (P17)

*“It is different when you have 2 professionals in the same sector compared to for instance consumers which would make it difficult for the legislator to objectively and prior to any case law to divide responsibility”* (P17)

[Who should be responsible for preventing this type of fraud?]

*“There needs to be more co-operation across various stakeholders”* (P8,P9,P10)

*“becoming a bigger problem and understood that this was a complex issue and required a multi-agency collaborative approach”* (P12)

*“Responsibility needs to be shared…”* (P14)

End User Education and Awareness

**Policy Specialists & NRA**

[As more businesses and users move over from legacy to next generation networks (or put in another way, legacy traditional communication networks to electronic communication networks) (NGNs), threats that were not necessary a problem on old legacy networking may exist in this new NGN way of running systems. Do you think a business should be made specifically aware of this kind of risk? If so, how?]

*“We acknowledge the importance of raising awareness and informing customers, including businesses, about telecommunications fraud. However, ultimately the customer would be responsible to ensure that any Customer Premises Equipment which is not within the responsibility of the electronic communications network and/or services provider (e.g. PBX) is set up in a secure way (e.g. using strong passwords to access PBX) in order to mitigate such risks to the maximum extent possible.”* (P4)

[Do you think the end customers should be made be aware of these threats?]

*“They should be made aware of the threats in the sense that people, especially the way I see it. There are 2 categories. There are the big companies, so if a company has a security department it never hurts to bring to their attention as part of threat intelligence, a new series of attacks or use cases targeting part of their infrastructure that they may have not paid attention to because they have a limited set of resources and were focusing on where the attacks were coming in.”* (P7)

[Do you think businesses should be made aware of this issue?]

*“Yes”* (P5)

[Thinking more broadly across the use of Electronic Communications Networks (ECNs). With all potential threats that exist, do you think Communication Operators (Phone Providers, Broadband providers etc.) should be open about risks that exist when using the internet?]

*“Various stakeholders including providers of electronic communications networks and/or services may have a role to play in educating customers on risks of potential threats when using the internet and on measures to be taken to mitigate such risks.”* (P4)

[Do you think businesses should be made aware of this issue?]

*“CP should make people aware so they are able to risk manage”* (P15)

**Lawyers**

[Do you think businesses should be made aware that their phone systems could be targeted and hacked?]

*“Yes”* (P19)

[So currently some providers are open about the risks and inform their customers what they can do to mitigate these risks. Do you think providers should be mandated to provide this information?]

*“Yes, however it’s one thing to inform, but it’s another to understand which solutions that should be taken.”* (P19)

[Building on what you have just said, do you think businesses should be made aware of this? For example if you do not setup your equipment correctly, you could get hacked and run up a large phone bill.]

*“Made aware by who?”* (P18)

[Their provider for instance, or some form of regulator intervention, some form of information campaign?]

*“I wouldn’t have any objections to a provider who choose to do so. I’m sceptical there is case for regulation compelling them to do so.”* (P18)

[Looking at the wider picture, should a service provider have more responsibility of the content for instance going through their channels or lines.]

*“Yes”* (P17)

*“I think we talk about 2 different stages which are both important. The information of the end user which is essential for educating them how to use devices...”* (P17)

*“For example, we’ve had to run a communication on how to use WhatsApp and how not to use WhatsApp for business purposes and how that has GDPR implications. People do need to be educated on that. For example, I did not know about this hacking, however through discussions I have now become aware of it.”* (P17)

*“I have been working in the IT sector for a long time, perhaps I am naturally more cautious using a USB stick, connecting a public WIFI, all those things that most people do not think about. I understand that I am a potential victim and am not sure if I am doing everything 100% right each of the time”* (P17)

*“So again, information is essential for the end user.”* (P17)

*“However, this layer of professionals they know what they are doing; I really hope so. So it is a question of how much responsibility can they take at that level, can’t we fraction that responsibility or if not call it responsibility, maybe requirements for each of them to make sure every time of the communication, somebody knows there is a risk and try’s to mitigate the risk. I think it would be foolish to think that we will prevent that completely.”* (P17)

*“I can say that the lawyer in me and my experience in a long career in the IT sector being on the side of the processor, so an IT supplier where our customer will ask us to have a bug free, defect free or guarantee 100% free security or guarantee they will never be hacked. This is ridiculous, this is not going to happen as we are always playing catchup.”* (P17)

**Cyber Security Specialists**

[As more businesses move over to next generation networks, do you think businesses should be made aware of the risks?]

*“Yes”* (P2) (P3)

[How do you think they should be made aware?]

*“That depends. This is a general cyber security issue so organisations likes the NCSC should take this up, because as with the general move to VoIP as being the standard, this is going to be an everybody problem. The provider should provide training materials, it doesn’t have to be full training material, but they could point to how to protect themselves.”* (P2)

[Do you think the provider should point out the key risks for using a specific service? For example, here are the key risks when connecting a PBX to our service. Just make sure you consider these. Something that gives them a bit of a chance. It is then up to them to educate themselves.]

*“Yes. So, in South Africa for instance, more people are being forced over to VoIP because of copper cable theft. They have a huge problem with home users, especially the elderly who not understand why they are being forced to use this technology. If you have small businesses who are having to use this technology and do not understand what is going on, there is a massive problem there. Back to the old thing of tick box compliance. Have people really given permission if they do not understand what they are saying. Are they in a position to say now? So why not put this on IPV4 behind a firewall?”* (P2)

[So, are you saying regulatory intervention?]

*“Yes, and possible not just education but encouraging the end user to take insurance specifically against this.”* (P2)

[Or even suggestions how they can protect themselves, such as by taking professional advice? This is what can happen, and you can take professional advice to help protect yourselves]

*“yes”* (P3)

[So, the question to where, I propose a back page of a bill, because it is easy. It could also be on their website.]

*“When you buy a fridge, it has safety information on the back of it. So what you’re saying is when they sign up to the service, they could be given some information in a leaflet for example. A safety information maybe.”* (P3)

[I initially thought of something like this, but it doesn’t necessarily deal with customers who have been a customer of a provider for a very long time and risks have changed. I am thinking of the customers who may struggle with technology. It’s the same or similar rules for consumers and small businesses in the communications sector.]

*“Maybe once a year as a reminder, I think that is adequate.”* (P3)

[So some form of information to the customer to give them suggestions once a year of what they need to be aware of.]

*“That would be something nice of the companies.”* (P3)

[Do you think the provider should be at least saying to the small business, using this new technology can introduce risks and you should lock down your equipment?]

[Explain to participant the UK and Netherland court case examples]

*“Interesting. Although I don’t think it is the providers responsibility to raise awareness around this point. I say this because if we look at just one Symantec suite for example. DLP package that they provide. If you install DLP on one of your end points and have it running and lets say you get caught via a phishing email, DLP tool would pick it up, but it was your responsibility to configure that DLP tool to ensure it gets picked up prior. It is your responsibility to ensure that Symantec suite is fully updated with the latest packages. So it is your responsibility as an end user to ensure that your Symantec is up to date and you have configured it correctly. If you get caught by a phishing email, I don’t think that will go back to Symantec to be their responsibility.”* (P1)

[*So it comes down to keeping knowledge and systems upto date and security by design?]*

*“Yes. My own organisation has recently only started communicating security by design for our applications to our leads. Security by design is a 30-year-old principle. So given that we are only reaching this point now and if we look at our competitors and benchmark ourselves against our competitors we’re probably not at the bottom, but also not at the top either. So it is quite concerning that when you don’t have the basic principles set in place, things with an emerging technologies aspect such as AI, robotics, block chain, VoIP etc. This is not going to be on our radar at all.”* (P1)

**IT Director & Trust Expert**

[Do you think that your provider should have made you aware of the risks?]

*“Yes, I think if I apply our own business model we sell our product and service, if there was risk of something happening to someone we are supplying a service too we would tell them about it and we would tell them that risk. We forewarn them. But yes, I think they should be making you aware.” (P16)*

*“I think the telco provider and any other party in the call chain for example Microsoft should make you aware of the risks”* (P16)

[Is this the only incident of its kind?]

*“Yes, we’ve had other attacks like phishing for instance. The thing is, your general user just isn’t aware. It’s the educational piece which is hard as people just don’t care. You know, you get techies who say here’s the problem and you have to end up trying to personalise it a bit. But every time we have a phishing attack, there is a bit of me that is worried that we have missed something.”* (P16)

[Do you think businesses should be made aware of these issues?]

*“I definitely believe they should be made aware”* (P20)

*“…I am not sure how much responsibility they should take for it and the reason I say that is because increasingly, especially since the GDPR came into effect. In 2016 businesses knew this was going to happen in 2018 and now everybody is so paranoid about whether they can use personal data for example, that I think there needs to be a bit of give and take. So that there should be at least an ombudsmen that looks at what is going on. Once you get into the data environment opposed to the copper wire. It was easy before to say their provider was responsible.”* (P20)

[Are you saying the provider should have more responsibility in informing the customers of the risks that could occur?]

*“Yes. Very much so.”* (P20)

*“…there needs to be an organisation like the ICO that needs to be a lot more helpful to the providers…”* (P20)

*“…as far as the GDPR is concerned, a lot of that is unenforceable from a data controller point of view. So people have these rights in Article X for instance and then an expectation in Article 30 that all the processes are in place to be able to support those rights. But nobody thinks about bringing it all together and nobody thinks about what the end user is really going to do. It has been known in the social sciences that around the internet, around privacy that people say yes we are really conservative and don’t like this, that and the other and then offer them free internet for a year and they will give everything away.”* (P20)

[Do you think providers should provide this basic type of advice?]

*“Yes, but they have to be very careful how they frame it.”* (P20)

*“For example, you get a broadband router from your telecom provider and they inform you it has a firewall, but they have to help people understand why that is important, especially as consumers.”* (P20)

*“And similarly for the small business opening up their PBX for whatever is out there, they need to understand what is going on, so there is no point in saying they offer this, that and the other.”* (P20)

*“The other thing is that people will become wary very quickly if there is a price to pay. Because the basic trust paradigm is between 2 people, but also works between a person and an organisation. For example, do I perceive it has benevolence, which does it have my best interests at heart, integrity such as doing a good job and is competent, it is capable of doing that job. That is the classic model of trust in the social sciences.”* (P20)

*“So as part of the benevolence piece I want my provider to tell me we are now doing this because we believe it helps you. We have been looking at what is going on in the industry and believe this is the right way. Immediately that makes me think they have my best interest at heart, they are not now trying to tell me I need to buy this new service, they are just telling me this is the way they are going to improve my service. They are competent because they know how to do this and they have integrity because they have intelligence, the technical know-how and have translated that in a way that I can understand which helps me as a customer.”* (P20)

*“It then becomes where in the food chain does that responsibility lie, but certainly if the providers are prepared to say we’re giving this away for free because we think this is the right thing to-do, that will start to strengthen the trust relationship in the user and the provider.”* (P20)

*“I see from a reputation and trust point of view that indeed the provider giving hints, you want to use this kind of equipment, you want to be careful if using this for instance.”* (P20)

**Ease of understanding**

[So, do you think there should be a list of threats which is published for each service type. For example, home broadband. These are some example threats that may exist. For small businesses using broadband, here are some example threats. For small businesses using telephony here are the threats for example where PBX hacking could be one of them.]

*“A list is a good thing for larger or professional players, but when you’re taking your home user, you can have a list at the back end, but at the front-end show something nice and show emotions.”* (P2)

*“Your right as what is needed is for the customer to understand in terms that are real for them.”* (P20)

**Contracts**

[Building off what you were saying before, it is going to be difficult for the provider to know what sector the customer is in. A customer could be a multinational company making many phone calls overseas, but another similar size customer may only be focused on the domestic market. In banking for instance, there is a lot of due diligence, you know what kind of organisation it is, their turnover perhaps and expected volume of international transactions. However, from a telephony stand point it will be more difficult as you cannot profile as easily. Do you agree with this?]

*“I agree, but I also think you can look at the regions which are being called. I think there may be other trends you can look at, but I think this will be a learning curve. Going back to your original point of should the supplier specifically raise awareness around this point. I think generically it will be raised in the contract. This is a control and it sets out simply what would happen for example that a customer is responsible for any misuse for instance.”* (P1)

[Do you think the provider should point out the key risks for using a specific service? For example, here are the key risks when connecting a PBX to our service. Just make sure you consider these. Something that gives them a bit of a chance. It is then up to them to educate themselves.]

*“If you have small businesses who are having to use this technology and do not understand what is going on, there is a massive problem there. Back to the old thing of tick box compliance. Have people really given permission if they do not understand what they are saying. Are they in a position to say no?”* (P2)

[Do you think providers should provide this basic type of advice? – After initial response in the IT Director & Trust Expert section]

*“…I have some sympathy with NEC. Any large business for whatever reason, they want to offload to another organisation, so is not so much a trust relationship, but a contractual relationship between them and so it is reasonable for someone like NEC to say KPN, you’re the guys running the network, so you should tell me. Then KPN come back and say we told you previously and you didn’t do anything. So then do NEC have to take a responsibility for their own staff, do NEC have to have a closer relationship with KPN? But before that specific scenario comes off, the expectation is that these guys know what they are doing.”* (P20)

Certifications and Accreditations

**Policy Specialists**

[I don’t believe so, at least in the UK, they fall out of scope of this]

*“It’s about the victim, not about the telco. So if this customer is an operator of so called essential services. Then we can consider, just like he should take appropriate technical, organisational measures that any IT system uses, although they should be identified as critical, but anyway the modern-day Caesar would also consider this as a cyber security threat. Finally, if it is a matter of these manufacturers or vendors suddenly digitalising or are stuck in the mindset of why would anyone hack us, haven’t implemented any reasonable security measures in their development procedures, then we can also make a case or consider whether to bring these kind of things to the attention of certification schemes or regulators.”* (P7)

[The person who setup the PBX or some other user, but maybe not even in a sense of misconfiguration, because they may think everything is setup perfectly, they were not aware of these specific risks.]

*“Misconfigurations of systems are nothing new. That is why in the Cyber Security Act it says any certified product must provide information of secure configuration and secure use to the customer. Just because something is hardened, it helps, but if someone takes a hardened system to be open, it doesn’t help.”* (P7)

[Asked participant if they were aware of any potential policy that could assist]

*“The new Cyber Security Act Framework could be of assistance with the new certification scheme, as awareness will increase in terms of what businesses are buying which will be delivered through the certification element of it.”* (P14)

*“the new Cyber Security act may provide some form of assistance through its certification scheme”* (P15)

**Cyber Security Specialists**

[So should small businesses be made specifically aware that their phone system could be infiltrated leading to a large telephony bill? If so, who do you think should inform them?]

*“If this is happening, then yes small businesses should be aware of this and it should be introduced in the Cyber Essentials Scheme. Because it is not part of it currently. If you look at it, every company has a telephone line. It makes sense to secure your phone. They have policies for bring your own device. They need to make the small companies aware of that. To do this though, you need to prove this is happening and can you do that?”* (P3)

[So you think there should be some form of guidelines?]

*“I think there should be some form of guidelines on how to do that. For example, I have been doing cyber security for about at least 10 years and I know very little about PBXs. If I have in the standard that tells me I need to do these things. Great it gives a starting point what to look for. Without it I don’t. Now lets say someone with 5 years experience was more than qualified to carry out some of the assessment with known IOS27001. This guy is not stupid, but he still needs guidelines on how to do this. The companies should again enable the customers to help with their own detection of this. If the customer needs statistics or some kind of thing, they should be able to provide it.”* (P3)

[Who should provide it exactly?]

*“The providers. So analogy is, if you buy a service from Amazon, you are responsible for that service. However, when you want to comply with something. They will give you the facilities, the tools to help you comply with the thing you need to comply with. With the new GDPR regulation, service providers are supposed to support the company when they are trying to maintain privacy of the individuals. They need to make special accommodations depending on the scenario for the customers to work with. This is as far as the companies should be liable for. Providing the capacities for the company’s to do their own analysis. To find out if they have been attacked and by how much.” [Who should provide it exactly?]* (P3)

[So, where would they get information if they have not heard of this?]

*“This is where you would have to look at one of the standards such as ISO27001, this would be a control, and this is how you would raise awareness. Organisations are typically ISO27001 compliant depending what industry you’re in. These organisations would need to incorporate this into their existing frameworks, and this would be the easiest way to raise awareness across the whole industry.”* (P1)

[So would specifically raise the awareness?]

*“So for example, looking at ISO27001, you would get audited in order to pass. Once the 2020/2021 standards get communicated, there will be a control in place for this that you need to have your infrastructure set in X place to Y standard. If you’re unable to do that, then you wont be able to get your ISO27001 certificate.”* (P1)

[What about smaller businesses that do not go down the ISO27001 route?]

*“So smaller businesses will look at NIS. It is not a regulatory requirement but is best practices. However, this would depend on the industry the company is in. For example, if the company is in the automotive sector then this may not be at the forefront. Their main intention may not be security issues. They may not have the frameworks set in place. So for businesses like that, then it’s really about raising awareness for security in general before you can get to this point. In terms though of who should own this, it is going to be a mixture of risk or compliance, but also the telecoms industry need to be the ones at the forefront of this movement.”* (P1)

[Do you think the provider should be at least saying to the small business, using this new technology can introduce risks and you should lock down your equipment?]

*“What they would say is that we advise the equipment you have in place would meet industry security standards. So, I think generally within the security space that’s an automatic benchmark, your environment needs to be up to industry standards. It is almost an unspoken rule or benchmark. For the provider to specifically raise awareness to that point I think it would be decremental to their business, I don’t think they have any obligation to provide that information. So, I don’t think the provider should be making them aware necessarily. Because your customer should already be aware of that and if you have industry standards set in place it won’t be a threat. In terms of a small business though I still think this applies because it is not the providers responsibility to be aware what your business is in terms of who they are providing services too. It comes down to you as a business and if you take a small business, security its probably not going to be in his mind at all. There are probably a tonne of vulnerabilities present in his system already, so going back to the responsibility. This is where I think it needs to be incorporated within something cyber security essentials framework or others such as NIS or ISO27001. So, if he ever does look at industry standards, he will be able to see what he needs to have in place.”* (P1)

[So PBX hacking for example arguable from a policy perspective is not necessarily a security issue, but more a service misuse issue because it is a trunk that has been provided and the that service is then being misused.]

*“This is a perfect example of why you see security taking a back seat in organisations and when you start pushing regulation. From a lot of perspectives, regulation and compliance becomes a tick box exercise and not actual security. It is a bare minimum. You see some organisations that are ISO27001 compliant but are not in the spirit of it and I think that is an ongoing issue, but that is something that has been going on consistently within the space. I don’t see any resolution. Initiatives of security or privacy by design being picked up, I see that more recently within industry and see that being picked up and applied to current standards.”* (P1)

[So if I am understanding correctly, what you are saying is presume the hardware or software is vulnerable and take the opportunities and transport links to it and disable them so you secure the network, you firewall the network so nothing can get to it?]

*“I think people focus on that element, on the transfer element, but there is a lapse in actually pen-testing that application. Which is something I’ve seen regularly. You can have firewalls at all your end points. That does not make you secure. That’s a tick box exercise to get ISO27001 certification, but that does not make you secure.”* (P1)

**Trust Expert**

[Do you think a certification program would assist and help? Or is it secure, but secure against what?]

*“Indeed, also the landscape changes all the time. You would have to recertify, but certification going back to the reputation thing tells you very little. It means we have just ticked that box and you see it in a trades body. So your local plumber is a member but it means absolutely nothing. It is much more powerful to have genuine recommendations, especially people you trust, because if you trust the person who is making the recommendation, that trust will transfer to the tradesman in that case.”* (P20)

Lack of Resources

**Policy Specialists**

[I mean that something to look out for so at least they know the need to protect themselves.]

*“How do they protect themselves, as you said that, you usually don’t spot it until you potentially get your phone bill which is then too late. You have 2 or 3 minutes during the weekend to shut it down.”* (P6)

**Cyber Security Specialist**

[Can you see how this increases the attack surface or vectors which make an organisation potentially more vulnerable?]

*“Definitely. So, if I take my industry, which is financial services, banking for example is quite mature in their security standards and generally what they have in place. If you look at the financial services space you’ve got insurance companies and wealth asset management companies also part of that industry and both of my experiences which in the present role is insurance as well as working extensively within the financial services space. I know for certain a lot of organisations will have this vulnerability present because we are still having issues with fixing core principles from a security standpoint. So, something such as unifying communications via voice over IP becoming a bigger and bigger factor. This isn’t going to be something that the organisations are going to be looking into in terms of setting controls to mitigate the risk or attack vector. So, I can see it being a large threat and I can definitely see it not being addressed in the foreseeable future. The only time I can see this being addressed or at least falling onto the boards radar is when instance occurs.”* (P1)

[So to confirm, you foresee the Financial Services Sector space only taking an interest when they are attacked themselves and run up a large bill?]

*“Yes. That is also purely based on when you don’t have your core principles. If we look at networks, for example, if an organisation who is producing billions of revenue on a yearly basis, in the insurance space or wealth and asset management space. If they haven’t configured their networks correctly to separate the DMZ or what applications are sitting where or don’t even have a CMDB, central management database for list of applications. If that is not up to date, which I know for a fact many organisations I have worked with this is the case. Something of this level is not going to be on their radar at all.”* (P1)

[If we take the BACS system. That system is very old and is still being used. There are probably lots of security vulnerabilities in it, but obviously it is heavily firewalled, and access controlled.]

*“There are multiple reasons for that, but one of the reasons is you are starting to get threats likes these which people are not aware of. There is not enough awareness behind them. This is going off topic, but if you look at block-chain, emerging technology, everyone can see the benefit from a supply chain perspective, but no one has realistically adopted it in the past 4-5 years. 1 or 2 banks have started to adopt it and there is a lot of proof of concepts and initiatives to push it forward and there is a reason why individuals are not adopting it and you can replace your supply chain from end to end, to have block chain technology and your cost efficiencies will be great reducing costs by 50-60%. You will probably have more on time packages, products etc. The reason it is not being pushed forward is because there is a massive cost element. The only output is cost efficiency. The board do not see that as enough of an indicator for investment to occur and you’re essentially doing the same job you had with your existing supply chain. That is one of the key reasons why you do not see the transition. At least in my opinion.”* (P1)

[Discuss current setup in sector and delay on getting real time information along with requirement for real time call connection and as little delay as possible]

*“So in that case you can situate the solution on the PBX itself.”* (P2)

[So based on our findings and how these attacks work, they attempt to infiltrate the PBX via multiple vectors including web portals]

*“Could you have a system that is on the same network, but not part of the box?”* (P2)

[There could be problems because many companies are unpredictable. On most occasion they may call one country, but then start calling others as part of their genuine business practices. Again, if you need to start adding more devices it can add further complexities as they will need to set it up.]

*“I’m talking about the volume of calls. If there is a delay for the service provider to find out what is going on then there is nothing they can do.”* (P2)

**ITD**

[So building off what you’re saying, in an experiment we conducted it was not just weak passwords, but also looking for vulnerabilities in the software.]

*“Doing port scanning, It is amazing what is left open and we have been very fortunate where we have had the investment. But I’m not saying we are not hackable. What you do as an IT director, you do the best you can and use the resource and money available at your disposal to mitigate as much as you can. That could be a strengthening of your perimeter, it could be locking down your cloud environment, it could be advance employment protection on everyone devices, it could be something sitting in the middle. You use whatever tools you can to put yourself in the right place. The challenge for people like me is getting that investment from the board and getting that investment from the senior management because all the time you’re doing enough to get away with it. You haven’t been hit badly, they put no value to you.”* (P16)

[Until you get financially hit?]

*“Exactly, till you get done, then they go. As an IT professional, you’re in a difficult place because if you fix everything, and you stopped getting hacked, you don’t get any investment. If you don’t get any investment, you leave yourself open to being hacked. Then you get asked why have you been hacked. It is a very difficult challenge. If you’re looking to invest money as a business or you’re looking to save money, do you want the IT guy to have it to make sure you’re more safe? No you want to invest it in new products, innovative ideas, stuff which is going to get your money rolling.”* (P16)

*“One of the key challenges for people in my position, how do you justify that investment, because actually a lot of it you could be accused of scare mongering because I’m saying if we don’t invest the money to tell us what is going on we don’t know.”* (P16)

**TPE**

[Do you think that smaller businesses would be more effected by this when compared to larger businesses? Because of their lack of awareness or capabilities for instance?]

*“Yes, I think there are a number of issues there. So, the small business does not have the resource to do all of these things and this touches on a point from before, where there needs to be somebody such as the ICO or equivalent in telecommunications is actually helping. But one of the big problems with trust is that a loss of trust for an SME is much more difficult and damaging than for a large organisation. It comes down to resources again. A large organisation is able to take the hit and then go through the process of rebuilding that trust. Such as holding hands, saying sorry, we were caught out, did not do it intentionally and this is what we are going to do to show that and we are learning from. A small organisation may just go under. You just need one person to successfully sue them for £500,000 and it wipes them out. But ironically people are more likely to trust an SME because it is not a corporate.”* (P20)

*“Which means both the SME and the customer are a higher risk and they do not necessarily share that risk because, as you say, the SME or small organisation just wants access to the features because that is what their business is based on. The customer will go along with them because they trust them and they know them. But they are more exposed and this is part of the problem with big organisations, suggesting that they are the be all and end all and they have their problems. But there is nobody out there other than the government organisations who will have the capacity to then monitor patterns above the individual customer level. So, you talked before about the dispute between KPN and NEC saying you have a duty of care to us saying this is not normal. But similarly, the government, or at least somewhere such as GCHQ or the NCA must see what is coming in and be able to produce a bulletin on a daily basis of these are the things we have seen.”* (P20)

[Looking at PECR and the use of the term significant threat can be open to interpretation depending on who it applies too. For a small organisation a £30,000 hack could be significant. But to a large company it could be we’ve been hacked, so data protection issues, so lets secure it and move it.]

*“Absolutely. Large multinational companies may not be aware that they have been hacked and this would just be statistical noise.”* (P20)

[I think the small SME in terms of responsibility may suffer from an unfair position because they have more responsibility in having to protect themselves from this when compared to a larger organisation.]

*“Yes, and smaller organisations are not necessarily in a position to-do that.”* (P20)

Trust

[So, building off the idea of the provider, providing a list of risks for a specific service being put on the back page of a bill, where the information was set by the EU, the national regulator or someone like the NCSC, do you think that could be a mechanism for informing?]

“*Yes. Although there is a specific problem with the NCSC, it is kind of a bad model because they were rolled-out of GCHQ. So, whenever you have a public facing entity that is still part of the state security apparatus, they have split loyalties. Are they defensive or are they aggressive? The NSCS is supposed to defend that national interest, but if they get a whiff of a new vulnerability, their first protocol is to kick it up to GCHQ and say, do you want to do something with this? That is a bad model. What you need is someone who is totally on their own and totally focused on defence. Something like that. But also, is well funded and would do the job. We don’t have something like that in the UK. Even if we did, the funding would always be an issue. So, I would be more inclined to go with industry bodies or companies themselves to have a duty of care to a certain extent.”* (P2)

[I’m aware of an incident where a PBX was hacked using a legacy trunk and were able to spend approximately £50,000 before their provider had become aware and then immediately informed them. This is why I think trust is an important line of enquiry as they claimed they were using a reputable PBX system and would not have thought this was possible. What do you think of reputation and trust in this scenario?]

*“I think your right. I think the way trust is built up and maintained is a lot more sophisticated than people realise. On one level you have your brand, and if we take it away from telecoms and think of the NHS for example, we see the brand and think this must be ok and then the day-to-day operation does meet up to our expectations. So the question then, is whether the overall reputation suffers or whether we as consumers or what other service provided under that brand are prepared to accept that things do not particularly go well. If we come back to a well-known historic brand. There is a presumption that you can trust them completely and implicitly. But, then the difficulty becomes the people with the very strong brands almost get away with almost anything because the reputation is so strong and also the social buys in or the community buy in to that brand is so robust and will just follow it and not make their own decisions and that’s part of the concern that individuals are not capable or not given the information they need to be able to make those trust decisions and will instead follow either the reputational press or everyone uses them so they must be good. Because I want to be seen as part of that set. Such as the iPhone. Unlike a lot of the engineers, trust is not about reliability necessarily and it’s not about cost benefit. It is about saying, am I emotionally and logically prepared to accept the exposure to risk in entering into whatever agreement? So, once you’ve got reputation in there, you then get an emotional response for the reputation. Once you get your peers or the group you want to be seen to be part of in there, then that has an enormous effect. So that is part of the reason why the NHS survives. It’s not because you have no choice, but it’s part of the UK psyche that health care is free at source and you can see it in the day-to-day operation doesn’t live up to the expectation around the brand. So, therefore people who suffer have got to look for a scape goat, so they will look somewhere else because the trust in the brand is so strong.”* (P20)

[So people would like to blame someone else such as not the brand, but the engineers implementation?]

*“Yes. The sort of risk which we recently saw with VW and the fiasco around emissions. So the question there is, was the loyalty to the brand strong enough to say, actually it’s the regulators fault for not being good enough. Which is a bit like the financial crisis. The regulator is not looking after us and actually we like the look of VW on the road. So, it is this kind of emotional response that gets things going and that is where the scams become particularly dangerous. Because you’re uninformed and the isolated who hear I represent this bank and then immediately the expectations are created in the consumer.”* (P20)

[To summarise and bringing the interview to a close, is there anything you would like to add or comment on?]

*“Two things. One which goes back to the policy makers, one of the problems with the EU and of course we have other things going on, we have fake news, we’ve got popularism. One of the problems is that policies are delivered on high and certainly around this kind of stuff, there needs to be more of an actual understanding of what people actually do and what people really understand and so it does matter whether it is me on the end my telephone or whether it is a large organisation or somebody in-between. There needs to be some real engagement with those people to understand what they really need. The other thing is, building off what we were exchanging earlier, If you get a contract in place, there is no need for trust. So, people will not necessarily be cavaliering what they do, but they will make assumptions, I have a contract in place therefore, I could sue this party if they get it wrong. So even with the NEC and KPN example, it is all based on law, but it is also based on the contractual relationship between the two. What we probably need going forward is to encourage a trust-based relationship and what I mean by that is there is more of an understanding that if something goes wrong, I have to sit down with the provider and say what do we do together. Yes, I expect my bank to pay me the money back if there is fraud, but it is more in this digital age, how do we work together so I get the best, but I understand what I am doing. In return I will not sue you because something has happened and I am jumping on a bandwagon and that seems to be the way to do it.”* (P20)

Liability

[As more businesses and users move over from legacy to next generation networks (or put in another way, legacy traditional communication networks to electronic communication networks) (NGNs), threats that were not necessary a problem on old legacy networking may exist in this new NGN way of running systems. Do you think a business should be made specifically aware this kind of risk? If so, how?]

*“However, ultimately the customer would be responsible to ensure that any Customer Premises Equipment which is not within the responsibility of the electronic communications network and/or services provider (e.g. PBX) is set up in a secure way (e.g. using strong passwords to access PBX) in order to mitigate such risks to the maximum extent possible.”* (P4)

[Europol published a Cyber Crime report where many of these frauds occur in developing countries going further to suggest that these frauds could be propping up failing states and governments.]

*“So my understanding is that the legal case that telcos bare direct and clear responsibility for this, doesn’t exist.”* (P7)

[As these attacks are highly sophisticated, do you think it is fair for the responsibility to be on the customers end in defending themselves against this?]

*“I don’t see it as being a functional possibility for the service provider to take liability. Because, if it is this large scale thing, then in the first instance it is not something the service provider physically controls, then it has to be the person who is physically in charge of the PBX system, the person who actually maintains it should be the one tasked with securing it. If you’re renting your system, that is a different kettle of fish.”* (P2)

[Do you think it should become a requirement?]

*“If the companies do that now, then it is coming from their goodwill, unless there is a case. I think what providers should do, which I think they do currently, is say what they are not liable for. They need to explain that these things can happen and they are not liable for this.”* (P3)

[So if we look at the banks for instance, they put a lot of checks in place to verify the authenticity of the transactions.]

“*I think that is from a liability perspective.”* (P1)

[Applying the same theory as in banks, do you think this applies to businesses? Especially small businesses?]

“*No, because this relies purely inside the customers infrastructure. You’re not reliant on the service provider. The provider is providing a service, but the point of vulnerability or exposure to be able to take advantage isn’t from the providers side. Now, if the provider was to implement some controls on their side which should typically be within their domain. So, if they are aware of this threat, is there something they can do internally? But in terms of setting controls or specifically raising this point to the customer. This is not something I would expect of them. Because 1) you need to know your customers business and that is not what their forte is.”* [Applying the same theory as in banks, do you think this applies to businesses, especially small businesses?] (P1)

[You wouldn’t necessarily need to know as they would have the technical capability to be able to setup that equipment.]

*“Not necessarily. There are so many end users and if we look at our organisation we have purchased the entire suite. Have we setup all of our products? No and that is not Symantecs responsibility. They can provide us support and they can provide us the workshops. But, if we do not have the capability or skill set from a security aspect to implement this from within our organisation infrastructure, the exposure and vulnerability still falls down on us. And this is talking from a global, multinational organisation. If we are not in a place with our vast infrastructure to get to a standard, given our situation that we are so large and complicated and there are various factors why we have reached this stage, but Symantec they won’t be liable if something happens to us.”* (P1)

[So you use their product at your own risk.]

*“Precisely. Typically, when you purchase a product, they will have a set standard informing you how you should plug it into your infrastructure. It will be quite high-level generic industry standard specifications. Now, if you do not have the infrastructure in place, that is not Symantecs problem. That will come down to awareness again. If your business is not aware, that comes down to regulatory.”* (P1)

[I think it’s difficult for communication operators to block correctly and as you found in your example with your provider, they sometimes get it wrong and in your case were overzealous.]

*“I don’t think they are responsible. If one of my users sets their password to something easy and they’re hacked and use the same password elsewhere as they use on their corporate email, you can’t be held responsible.”* (P16)

[Should providers be completely responsible?]

*“Against total responsibility as it could encourage negligence (e.g. if one party had total responsibility, then it could encourage the other party not to set their systems up correctly)”* (P17) *(notes from follow up with participant)*

[Should providers have any responsibility?]

*“We didn’t bother to do anything upfront, we could have found that document but didn’t even think to look. Someone else should have been responsible for telling us about this despite the fact we choose to do it ourselves.”* (P18)

*“If you put it in a different context, no one told me if I didn’t service my car it might go bang. If someone did, it would have been different. Or, no one told me if I went and did this illegal thing I could be prosecuted for it. Perhaps the onus is on you to go and find these things out.”* (P18)

*“A business should investigate risk”* (P18)

*“When something goes wrong, it is very easy to point to someone else and say you should have told me about it. I’d be curious to see what their contract with their SIP trunking provider said about security”* (P18)

[I think that would be a very good question.]

*“If it is one that I’ve written, it will say quite early on, upfront they are responsible for the security of their PBX. They are responsible for the toll charges associated with fraudulent use or use that appears to generate from their network. So, even if it doesn’t tell them how to fix it or what to look for, it’s quite clear in pointing out there are security risks and this is on them to mitigate them”* (P18)

[Due to the nature of these attacks do you think it is reasonable for all of the responsibility to be on the small business customer to protect themselves?]

*“No”* (P19)

“So, in your research area, I’m not saying there is a duty of care or rule to suggest in these specific set of circumstances, but generally, it not unusual to have a duty of care applied on a service provider as you’ve got that in other contexts.” (P19)

[I was just wondering for example here in the UK for instance, if there is anything you can think of exactly directly states, rather than implies.]

*“I can’t think of anything, I don’t know if there is cross sector, whether negligence is of any help, but there is a contractual relationship between the provider and the business.”* (P19)

[Where I guess it would come down to what is in that contract?]

*“Exactly”* (P19)

Growing threats and IOT

[For example, it could be putting procedures in place such as everyone who wishes to access the unified communications network, needs to use a VPN to access to it. So many organisations require teleworking.]

*“Sometimes you have a novelty, in the sense that people get on board. People I follow on twitter, they go on board a ship and discover all kinds of old legacy connections that nobody knew were connected to the internet. The novelty is either in the vulnerability which can be in the setup and bad administration and of course, the mitigating measures are not novel. However, in your case and from my perspective, the novelty is in the fact that somebody is abusing a PBX, that I hadn’t thought of before to make money, now the mitigating measures seem the traditional mitigating measures, so the suppliers could put in effort to make their things less prone to abuse, there is a component of user awareness to take of this.”* (P7)

[Essentially information that is put on the back of their bill, so for example if the regulator were the body to create the graphics and information, the back of a phone bill becomes used by the regulator to inform the customer of the risks. It is up to the customer if they decide to turn over and look at it, but it could be one of many ways to educate the customer.]

*“Exactly. There will always be the more sophisticated things that you won’t be able to mitigate against. But you should try to mitigate against the common things as they happen 80% of the time. So, crowdsource pen testing. I was discussing previously with someone about this and they were saying oh, are these guys looking for zero days and something similar? No, they are looking for badly configured services, if someone has forgotten to set a password. Really stupid things which happen all the time. If someone hacks your password, it’s not because they are a super hacker, but because they have a password list that is published. People reuse the same password. No matter how big the company is, it is still the end user that sets the thing up. Maybe they don’t know what they are doing or have 10 different people working on the same thing. One person has setup it up one way, and another person has set it up in another way. You create a disparity that shouldn’t be there and hackers will always find a way to exploit that. I guess it will be the same for a PBX.”* (P2)

[To summarise you believe customers should be informed of potential threats and how they could mitigate them, but how, that is still to be determined?]

*“Yes, as you would do for a fire for install, such as a risk analysis, you should at least inform the user. The reason why it is not as obvious as a fire, as fire is safety, while attacks that we mostly see are just security. When one of these IoT devices can kill someone, then it becomes a safety thing. At that stage, it should be mandatory to provide this information.”* (P3)

[There are systems in place, but they are not very good and heavily rely on post detection. It would be difficult if a provider blocked a country and a customer had to phone up to get it unblocked.]

*“I think with time this is where you can start looking at trends. Noticing how you can implement controls and in what areas. I think it will be a learning curve for the industry given this is a newish, growing threat.”* (P1)

[Discuss IPv6]

*“I think that is why you have not seen the industry shift yet.”* (P1)

[So going back to the awareness point, do you think the provider should be saying to the consumer that they need to keep their stuff up to date? So essentially where should the awareness be coming from?]

*“I would go back to the regulatory again as awareness, but I’d also go more importantly looking at the whole concept of IoT. The age we are moving into there is very limited regulation around that area and that is a key issue with many people having Alexa at home, having a smart doorbell. The benefits are there, but increases lot of risks, so what I would like to see in the space is before you launch a product or service, there needs to be a conversation in the space in terms of the impact. There needs to be some independent aspect from the regulators to come and try to pen-test your product, to come and see what vulnerabilities exist.”* (P1)

[There is never going to be 100% though.]

*“You would never get it to be 100%, and that is where we see we have a constant stream of updates.”* (P1)

*“This is where updates need to be automatically pushed. If I look at my internal structure of the organisation. We’ve got 12,000 employees. We don’t give them a choice to update their laptops. If we have a key patch update, it gets done. Be it over night or wherever it gets done in the background. I think the same approach needs to be taken for critical security updates. Otherwise, we will be in a situation where the customer has no control. In terms of generic updates, for ease of accessibility which contain new features that should still remain a choice. But key security updates should occur in the background.”* (P1)

[So it comes back to the vendors then?]

*“Yes”* (P1)

[However, if you consider some devices which are made, they are produced, never to be updated again.]

“*True, but for the main players and main consumer market, there is ongoing service. For critical security updates such as push updates to your router, your fridge or other device we don’t do so much automatic pushing.*” (P1)

[So do you think the responsibility completely falls on the consumer?]

*“Not necessarily, the responsibility of ensuring my phone or device which is publicly facing to the internet. That product for security aspects, I see the responsibility being from the vendor. They need to ensure that the device is secure.”* (P1)

[So if we expanded this onto the business side and back to telephony, would you say the PBX manufacturer such as X for instance has the responsibility for make the product secure?]

*“Yes. It is the vendors product, the vendors device, it is the vendors responsibility to ensure the security updates.”* (P1)

[Then you also need to look at how much control a customer has of that product. With a PBX for instance, the customer will most likely have a lot of control to configure, but with a IOT device they probably have little control to configure it. So, in that case would you say it is the customers responsibility or the vendors responsibility?]

*“In the first instance, if a vulnerability becomes present because your infrastructure is not up to date and is not configured correctly. There is exposure. In the second instance where we are looking at a device specifically, my phone for example. My vendor automatically sends security updates which occur in the background. If for some reason my wireless network does not have a password or it is not configured correctly because I have gone in and played with it and someone is able to exploit that and gain access to my phone, that doesn’t come down to the vendors responsibility. The point of intrusion is not because of the vendor. If you have an exposed web interface, port scan, SQL etc, so to me that does not come down to the vendor as long as the vendor has ensured that the latest security update or patch for their device.”* (P1)

[Were you aware that next generation Public Electronic Communication Networks could be used to steal this volume of money from businesses?]

*We understand that the threat of telecommunications fraud increases in next generation networks.”* (P4)

[As more organisations move over to next generation networks, can you see this becoming more of an issue?]

*“I suspect if people do not continue to secure their equipment, then I suspect it will, yes. There may be things telcos could do within their cores to try and be better at spotting unusual traffic. To the extent the telcos are subject to a regulatory requirement to do so or they are suffering financially themselves if they are left in an arbitrage situation. Maybe more needs to be done within the telco network itself”* (P18)

[On this topic, where attacks are today, compared to 10 years ago, they have increased. In the home environment where we have smart homes, many attacks today are being conducted through smart devices such as TVs, DVD Players etc. all because they have this smart element in it.]

*“That is only going to increase”* (P17)

*“Relating to Bring Your Own Device, its difficult because it’s their own device you want to give them their own privacy and freedom of using that device”* (P17)

*“Would we agree for professional contact information stored in outlook to be used by a chat application?”* (P17)

*“Such as WhatsApp, Viber, Telegram, WeChat as we have business all over the world including in China.”* (P17)

*“That’s exactly the problem as we are still controllers of that information. Whereby in theory WhatsApp will be our processor, but we both know we have no control over what WhatsApp is going to do with that information.”* (P17)

*“Bring your own device when it comes to security, I found is very difficult and increases the risks and unfortunately if you give the hardware away, opposed to bring your own device it would be a policy by which the company gives you a device and since we are talking about electronic communications you cannot possibly not be tolerant to a certain degree with personal use. So we are again in the same kind of risky situation”* (P17)

*“Could see issues around privacy, which could potentially see issues in the service provider looking at details into this.”* (P17)

[Can you see how from a security perspective this can introduce new attack vectors and increase the likelihood of getting hacked?]

*“Indeed. Yes, very much so. I think people are very naive about it. Once it comes in on a data channel, that could effectively give it access to anything.”* (P20)

[You could simplify and say it is an internet connection.]

*“Yes. People may not understand IoT, but they do like the gadgets. It is fairly trivial to order an extra basket for the fridge. But nevertheless the same mechanisms are there.”* (P20)

[What do you think could/needs be done?]

*“Responsibility needs to be shared and processes could be needed to be implemented to create security by design (similar to privacy by design). This may require further regulations. This could be especially important where threats are continually evolving.”* (P14)

Policy

[That is based on looking at the previous working and looking at how member states implemented the Framework Directive and Article 13a.]

*“So, assuming the telco doesn’t have such systems in place for their customers, the actual confidentiality, integrity and availability of the network has not been compromised. For it knows there is a valid call placed from this PBX to Mr Jones in the Republic of Congo. So it is hard to say from a legal and strict interpretation of their duties that they are failing their customers, based on the Code, unless the Code has provisions for preventing fraud, which I am not aware of.”* (P7)

*“This is the difference because there was no definition of security in the Framework Directive and member states more or less agreed in general it is mainly the uptime. It’s mainly about the availability we need to focus on. But with the new code, it’s the full range of confidentiality, integrity and availability. So this is a big change.”* (P6)

[Aware of other policy that may be applicable in relation to this type of fraud?]

*“I would like to refer also to Art. 97(2) (which largely corresponds to Art. 28 USD), whose scope of application, however, has been extended (due to the reformed definition of electronic communication services in Art. 2(4) Code)”* (P11)

[VoIP technology has been around for over 10 years now. However it is now only in the past few years are companies transitioning is because they are being forced as by 2025 there lines will be turned off.]

*“I think the exposure, responsibility, accountability and liability sits on the vendor to make sure your environment is ready. But on IoT, that comes down to again it is your responsibility to ensure your environment is secure, but at the end of the day what I would like to see is if a specific product is vulnerable vendors do not provide you a choice and automatically push.”* (P1)

[So the vendor takes responsibility for protecting and securing their device?]

*“Yes. For their own infrastructure. [vendor takes responsibility for protecting and securing their device] There may be another factor where you have policies in place. However, in reality if you look at any organisation, especially a large multi-national organisation, there is a massive disconnect between policy and procedure. You can have an amazing policy written up, but in terms of individuals following it, it is something you may not see in the space.”* (P1)

[If you look at the Code, it is very similar to what was in the previous telecom Directives.]:

*“Yes”* (P5)

*“Article 40(1) of ECC is 13a”* (P18)

*“Article 40(3) of ECC questions whether this would reach the threshold of significant risk”* (P18)

[It is the customers equipment or account that is misused. Therefore, service misuse.]

*“Regarding state of the art, is there anything the provider could be doing to mitigate or prevent?”* (P19)

[State of the art is subjective, when you say state of the art, do you mean e-privacy type definition?]

*“No, I mean technical state of the art, so if I am the provider and I notice this is happening, can I do anything?”* (P19)

[Potentially block it, analyses, inform the customer]

*“Are these solutions not too expensive?”* (P19)

[So, to summarise, you think it is unreasonable for the customer to be solely looking after themselves. Even if they are a large organisation? Or do you think large organisations should be treated different compared to small organisation?]

*“I would get insight from an expert to understand who is best placed to do something. Obviously in terms of capability, who has the capability therefore to implement the mitigating actions.”* (P19)

[When you mention duty of care. Are you aware of anything statutory in law in regards of duty of care? Or are you saying this as generally they should have the best interest of their customer?]

*“Providers can have different types of duty. If I take an analogy here, content regulation for example, some service providers have a duty of care which means implementing filtering of screen content and to make sure, to the extent possible.”* (P19)

[In that example, would that apply to businesses? Not just consumers?]

*“I do not know about the threshold, but when it comes to small businesses, maybe. It is also a matter of understanding. If you are a big business, what would you do to prevent this from happening?”* (P19)

[Inform about the NEC and KPN issue]

*“So in your research area, I’m not saying there is a duty of care or rule to suggest in these specific set of circumstances, but generally, it is not unusual to have a duty of care applied on a service provider as you’ve got that in other contexts.”* (P19)

[So an issue that I am finding is that businesses do not know they need to protect themselves against this.]

*“You could see the insurance industry developing on this, but that will require them to identify that this is happening. At the minimum, if there is one party that has the key to information and could inform, that is the service provider.”* (P19)

[Explain boundaries of a public and private Electronic Communications Network]

*“The distinction here is distinguishing between a private and public network. It is a matter of scope.”* (P19)

[Do you think providers should profile the key risks and inform their customers, these are the risks that could happen if your service is misused?]

*“Yes, they should do a risk assessment for example, but at this stage I don’t know what that would fully require. However, if you provide a service and there is a high likelihood of me misusing the service, then there is something wrong here.”* (P19)

*“One which goes back to the policy makers, one of the problems with the EU and of course we have other things going on, we have fake news, we’ve got popularism. One of the problems is that policies are delivered on high and certainly around this kind of stuff. There needs to be more of an actual understanding of what people actually do and what people really understand and so it does matter whether it is me on the end of my telephone or whether it is a large organisation or somebody in between. There needs to be some real engagement with those people to understand what they really need”* (P20)

Member states, NRA & other competent authorities

[I would not say it is like this in this scenario]

*“From a policy / regulatory / whatever dimension, in the paper you sent us, you have identified and speak about the Code. Because the Code refers to the responsibility of the telcos. As you correctly said, it’s a question of definitions and who is responsible for what, but then I’m curious for example, is there a dimension of police cooperation, do the authorities or regulators in those receiving end countries bare any responsibility?”* (P7)

[Who do you think should be responsible according to policy?]

*“Also note that the Code is a Directive (as is the current legislative framework), which has to be transposed into national law by the Member States. It is for them to follow-up on the issues mentioned and also the expertise and practical experience with the daily application in practice and the combatting of fraud lies with the Member States and their authorities.”* (P11)

[Who do you think should be responsible for informing?]

*“NRA’s have the responsibility to inform of these kinds of issues”* (P15)

[How do you think they should be made aware?]

*“That depends. This is a general cyber security issue so the NCSC should take this up, because as with the general move to VoIP as being the standard, this is going to be an everybody problem.* *The provider should provide training materials, it doesn’t have to be full training material, but they could point to how to protect themselves.”* (P2)

[So following on, where do you think responsibility should be in terms of protecting the customer? Do you think it should be the businesses responsibility, the operator or the regulator?]

*“Regulators should do more work because you cannot expect the service provider to protect all customers. I do not see that being practically applicable.”* (P2)

[Can you think of any policies or legislation either UK or other EU member state that could be relevant to this?]

*“Outside the normal criminal stuff such as the Computer Misuse Act and fraud, no”* (P2)

[Do you think the communications operator should be more open about the risks when using their service?]

*“Yes”* (P2)

*“I think with all that is going on you have a regulator that is removed from the end customer. The regulator targets the service provider, the service provider is incentivised by selling and not by informing and for the service provider, informing of all these risks, frontloads the possibility that somebody isn’t going to buy the thing.* *So there is a disconnect that needs fixing . When you get organisations like the NCSC, they are trying to do education, but they do not have funding or money to do it. Not to the extent it needs to be done.”* (P2)

[They are not working with the communications operator and could argue they are having to do a bottom-up approach.]:

*“Exactly. It would also be cheaper for service providers to provide that kind of education because you only need to prepare those materials once. So for them to do it, they have massive reach. Do it once. But they could also do it via an industry wide body.”* (P2)

[So globally could you guess how much?]

*“I don’t know, but I reckon I could find out because the UK has national crime statistics which has some figures which could give me an indication. With that, if I have that piece of information and I know which key words to look out for I could probably find that information.”* (P3)

[Do you think businesses should be made specifically aware of this kind of risk?]

[By who?]

*“The same people behind cyber essentials*” (P3)

[Not the regulator, the communications operator?]

*“No, it should start at the police station because police stations collect information about cybercrime that happens in the UK”* (P3)

[Like Action Fraud?]

*“Yes. This type of fraud needs to be reported. If someone is being cyber bullied or blackmailed over the internet, they need to report it.”* (P3)

[And you believe it should be local police organisations who should be educating?]

*“Yes”* (P3)

[Do you think their own service provider should be making them aware? If so why?]

*“No, because they give you a service, they are not responsible for your privacy or security. How you take care of your phone is your responsibility.”* (P3)

[Would you say they are sophisticated?]

*“Yes”* (P3)

[Given the sophistication of these attacks, do you think it is correct that all the responsibility should be on the customer to protect? Do you think the service provider should still be monitoring the patterns and profiles of usage to look for any misuse? Similar to the Financial Services Sector.]

*“The service provider should be able to allow you to maybe detect these types of attacks or help you comply with something, for example, where it says if you have a PBX you need to comply with this, this and this.”* (P3)

[Do you think they should be forced to do that?]

*“I don’t’ know. I think it should be the government who do that rather than adding another overhead for telecom companies. Yes, they make a lot of money, but you also pay taxes for the police.”* (P3)

[Is it effective?]

*“To ask the police to go and inform the public about these dangers. It is their responsibility. If you try to force the companies to do it, you are moving the responsibility from the official government body who should be doing this, to a body who should not be doing this. Also don’t forget, the government is actually trying to do an export control on the licences that come into the country to make sure it is compliant.”* (P3)

[Do you think a provider should say to there customer that they need to keep their equipment updated and secure, because if not, this could happen.]

*“From a regulatory standpoint, I don’t think they should. However, I think there does need to be an initiative around this or at least some awareness around this.”* (P1)

[How do you think this could be done?]

*“Your internal security department. Whoever is responsible for setting up your infrastructure, dealing with the connectivity aspect.”* (P1)

[So if I’m understanding correctly, your saying that if anything was going to be done, it should be via a change in the regulatory framework to make customers aware?]

*“Yes. And that is the whole point why you have organisations meet with the regulators.”* (P1)

[So would you say a communication provider providing to a consumer should have a duty a care to their customer and make them aware of the risks?]

*“In this scenario, it is not as simple. It still comes down to the communications providers fraud teams looking at this. They may need to bulk up the controls, their protection.”* (P1)

*“I do think the legislator, at the European level is much more accurate nowadays and makes more sense. There are things that Europe shouldn’t be busy with, but there are other things that really make sense to bring up at the European level. There are other issues that make sense to be sorted, or at least thought of and policies put in place at the European level first. This type of hacking knows no boundaries. So, why don’t we consider seriously, what could be the requirements for each actor and see what the specific stakeholders and actors can do at their level.”* (P17)

[When you say yes, do you have any thoughts of how this could be achieved?]

*“By regulators”* (P19)

[What about there providers?]

*“As well for sure, yes.”* (P19)

[Are you suggesting the regulator should be taking more responsibility? Such as informing customers and users? Arguably an impartial view?]

[So do you think the regulator should be taking a more active role or participation in making users aware?]

“Yes” (P20)

[So are you suggesting people do not appreciate the value of their data?]

*“No, indeed. So, I think it is unfair to suggest the carrier or the service provider has to take complete responsibility. You have an actor network essentially. You have your regulator, but you also have your end users and the service providers. We can’t expect the service providers and end users between them to do everything to make sure everything is secure.”* (P20)

[Building off that, would you say that there could be a bias or conflict of interest if the provider decided what was best for the end user?]

*“Yes”* (P20)