# Transcript

## Section A

00:00:02 Interviewer

Okay, so next we are going to interview TPR2 from [a private company].

00:00:10 Interviewer

I'll start with section A and ask you the first question. You are at a private network security provider, right? Yes. And the second question is, where do you work?

00:00:24 TPR2

I currently work in the IR team in the Taiwan BU.

00:00:31 TPR2

The IR team stands for instant response team.

00:00:34 Interviewer

Is it in ?

00:00:35 TPR2

We investigate incidents, for example, when a customer has a problem, and they wonder why their environment was compromised. We send someone to check their computer on site and find out where the intrusion came from. Then, we help them identify suspicious samples and information, analyze them, and provide them with solutions for defense.

00:00:57 Interviewer

Hmm, I see.

00:00:59 Interviewer

Do I understand correctly that the name of your department is IR team? Can you tell me again?

00:01:04 TPR2

Yes, the IR team, instant response.

00:01:08 Interviewer

Okay, got it. Now, about the following questions...

00:01:12 TPR2

I think that's it.

00:01:13 Interviewer

Oh, it's okay.

00:01:14 TPR2

Actually, this department... well, it didn't exist at first. But our supervisor, who is currently my supervisor….

00:01:27 Interviewer

What supervisor?

00:01:28 TPR2

My current supervisor. Yes. We used to belong to the support team in the Taiwan BU, but then they thought that IR was a growing trend. So, they created the IR team under support. I've been here for a while, but the unit itself has only been around for about 8 years.

00:01:47 Interviewer

I see, 8 years.

00:01:49 Interviewer

How long were you in your previous unit?

00:01:54 TPR2

About 4 years.

00:01:55 Interviewer

4 years.

00:01:56 TPR2

I've been with [a private company] for over a decade now, though.

00:01:57 Interviewer

So you've been with [a private company] for over 10 years?

00:02:01 TPR2

Yes, but this department I have been in around for about 8 years.

00:02:04 Interviewer

8 years is quite a while, though.

00:02:07 TPR2

Yes, it is.

00:02:10 TPR2

My current position is as a consultant, specifically a cybersecurity consultant. Whenever we go out, we all refer to ourselves as consultants. Our main responsibility is related to cybersecurity, and we handle a variety of tasks related to it.

00:02:22 Interviewer

So you say that you're consultants? Okay, cybersecurity consultants.

00:02:26 TPR2

Our main responsibilities currently involve everything related to dealing with cybersecurity.

00:02:35 TPR2

For example, we have two major services. One is what we call IR, where we go to the site to investigate, collect samples, and provide a report to the client on what happened, how they can defend against future attacks, and how they can improve their environment. If the client is interested in making significant improvements to their environment, we also provide consulting services where we interview people in their environment to identify areas where they are not doing well.

00:03:08 Interviewer

I see.

00:03:13 TPR2

So, we will assess aspects such as the placement of components in your setup. For example, if you have an Active Directory (AD), a firewall, a Web Application Firewall (WAF) behind it, and maybe an Intrusion Prevention System (IPS) at the back. We will analyze whether the placement of these components is correct and whether they are effectively leveraging their strengths. After the assessment, we will provide you with a report detailing our findings and recommendations for adjustments to enhance the security of your environment. This is just one aspect of our services.

00:03:41

Okay.

00:03:43 TPR2

The other part is called monitoring.

00:03:46 Interviewer

Monitoring?

00:03:46 TPR2

Currently, we have many information security products, but customers may not understand them well. They need extensive training to understand how these products work.

00:03:59 TPR2

So, instead of customers spending a lot of time on training, they can buy our services. After customers purchase our products, we will provide them with monitoring services. We will directly monitor the logs and notify customers when there are events or problems with their computers. These are the two main services we provide.

00:04:16 Interviewer

Ok, got it.

00:04:21 TPR2

It’s our department’s job, we are responsible for...

00:04:21 Interviewer

Ok, your department. Can I have your business card later?

00:04:25 TPR2

Sure, you can.

## Section E

00:04:27 Interviewer

Okay, then that’s all for section A. After that, we'll flip to section E, which is more related to network security and your functions. Section E mainly focuses on overall network security. For example, the first question is about…

00:04:55 Interviewer

Based on your understanding, what are the major network attacks that Taiwan is currently facing, and the methods used in these attacks. Can you give some examples?

00:05:08 TPR2

Well it’s difficult to enumerate all of them.

00:05:16 Interviewer

That’s alright.

00:05:17 TPR2

Because there are just too many scenarios, currently in Taiwan, it can be divided into two or three categories. Facing attacks, well, this question is too broad and needs to be more specific.

00:05:29 Interviewer

Too broad… yes, I mainly focus…

00:05:30 TPR2

Yes, yes, yes, for example, when we face attacks, actually, we can divide them into two main categories. One is from China, which is the majority, because China had many attacks in the past years, but recently, it has decreased a little bit, but I think it might come back again because they are reportedly going through some reorganization, so they have been less active in attacking us, but recently, they have come back. The other side is the so-called cyber hackers, the general ones, and recently, ransom attacks are the most common. Most of the attacks are ransom attacks, and the others are relatively less common.

00:05:56 Interviewer

I see.

00:06:00 TPR2

We also divide it into similar ones from China but relatively less common, and then divide it into these three types, which are the majority. Probably these three types, and the others are very specific, so we mainly face attacks from China, then ransom attacks, and then other minor hackers.

00:06:18 Interviewer

What did you say the second one was just now? China?

00:06:19 TPR2

Ransomware, oh and China's cyber army, they are specialized in collecting intelligence.

00:06:20 Interviewer

Hmm, China's cyber army, and then?

00:06:25 Interviewer

So they... they should be sent by the government? Or not necessarily.

00:06:29 TPR2

Most of them are sent by the government, but there are also private ones, yes, there are private ones. The ones sent by the government are very obvious, you can tell which faction they belong to from analyzing the malicious programs and the characteristics inside. You can know which region of China they are from based on that.

00:06:44 Interviewer

I see.

00:06:46 Interviewer

So you mentioned China just now, and then the second one was?

00:06:49 TPR2

Ransomware, yeah, it's like extortion software.

00:06:53 Interviewer

Oh, oh, I see, I see.

00:06:55 TPR2

Basically, in the past two years, 2021 and 2022, ransomware has been the most common threat in Taiwan. They encrypt your files and demand money from you.

00:07:02 Interviewer

Hmm.

00:07:10 TPR2

And this kind is the most common in the past two years, and there is another type, and there is another type which is known as stealing personal information. The one stealing personal information is more like a smaller...currently considered a minority, and they target e-commerce platforms, yes. However, the second type and the third type may overlap, meaning that after stealing the information, they may engage in ransom attacks, depending on which category they belong to, yes.

00:07:33 Interviewer

Okay. Have you dealt with the WannaCry incident from 2016 before?

00:07:39 TPR2

Yes, yes, it was very devastating, and it should be said that the handling was not complete, and there are still unresolved issues until now, yes, because at that time, people didn't know they had to apply the patch. The WannaCry ransomware, in fact, exploited a vulnerability.

00:08:02 Interviewer

Oh, a buffer overflow attack?

00:08:04 TPR2

No, a vulnerability exploit.

00:08:05 Interviewer

What's that? Oh, sorry, I didn't hear that clearly. Vulnerability exploit, okay.

00:08:06 TPR2

Vulnerability attack, and it's this kind of thing that most of the time cannot be fixed, especially in the production line, most of the time they cannot be fixed. So when encountering this thing, the production line is usually the first to be completely affected, and at that time, it's basically impossible to save everything.

00:08:30 Interviewer

So it's not possible to fix it?

00:08:34 TPR2

Because it's a unique industry, the machines used in production lines are very old and cannot be repaired.

00:08:41 Interviewer

Oh, hmm.

00:08:42 TPR2

Because they dare not touch the things inside, some of them didn't even sign for maintenance, so they cannot fix it themselves. In case they try to apply a patch and it breaks, their machines will be down, and they won't be able to recover them. Also, they may not have a vendor to help them, or they would need to spend a large amount of money to fix it. Stopping the production line is something IT absolutely does not want to happen, so they rarely apply patches. Due to this reason, the problem can spread extensively, and after getting in, everything might be affected within a week. Yes, that's right.

00:09:18 Interviewer

Hmm, I see.

00:09:20 TPR2

This has been going on for a long time.

00:09:22 Interviewer

Yes, that was quite a long time ago, and it's famous because almost the entire world was attacked at that time.

00:09:31 TPR2

Yes, that, that because it is an automatic expansion, so basically, if it is not fixed, it will, it will, it will be affected.

00:09:38 Interviewer

OK, got it.

00:09:41 TPR2

As for the network attack methods, this is a bit extensive, it's more like, um, it should be said that they change every year, they change every year, and the previous ones, um, the methods, it's not easy to discuss.

00:09:57 TPR2

Um, let me just explain this generally. If your environment hasn't been compromised yet and it's still in a clean state, hackers usually start their intrusion attempts from two or three entry points. One is your email, then there's your website, and the third is the external services you provide, like RDP (Remote Desktop Protocol) service or other remote desktop services like Citrix. These three points are the most vulnerable to breaches.

00:10:27 Interviewer

I see.

00:10:29 TPR2

And there's the fourth and fifth ones. The fourth one is usually attacks from suppliers or third-party entities that may not have a direct relationship with you, but they have some commercial interactions or indirect connections. As for the remaining five, there are many, and they are less common, with the majority of attacks focusing on the first three entry points.

00:10:48 Interviewer

I see.

00:10:49 TPR2

So what techniques do they use? Usually, they send a lot of social engineering emails.

00:10:55 TPR2

f I'm not familiar with your environment, I'll start by testing it. I'll send social emails and try to get you to click on them. If that doesn't work, I'll launch a direct attack on your web server. Yes, and there are also direct exploits of vulnerabilities. I'll check what type of web server you have. For example, if you're using IRS or Apache, I'll target known vulnerabilities for those web servers to attack your website. Moreover, if you're using certain packages or plugins, they'll search for them. For example, there is a package that is commonly used, but I can't remember its name right now.

00:11:24 TPR2

Oh, I also forgot the name. Um. Um. I forgot its name; it's a very commonly used package for building websites, a simple website building package. It has many vulnerabilities, and it's often targeted for attacks. It's usually easy to exploit and take down.

00:11:40 TPR2

Hmm, and the third type I just mentioned is, for example, RDP (Remote Desktop Protocol) services. Nowadays, there are many remote working setups where people can connect back to the company's network from home. They use RDP to access internal resources. However, sometimes before entering, they may only have username and password authentication, which is easy to compromise. If there is no additional security like two-factor authentication, attackers can directly access your environment through this entry point. So these three are the main entry points, and most of the investigations we have conducted show that attackers enter through these three entry points most frequently.

00:12:19 Interviewer

I see.

00:12:20 TPR2

Most of them, there are too many details inside. The entry points are mainly these three, and the third one was the biggest last year.

00:12:29 Interviewer

The third one was the biggest last year. In 2022?

00:12:33 TPR2

Yes, because everyone was working from home, and everyone had to set it up, and then they wouldn't pay much attention to it, so it was easily hacked.

00:12:39 Interviewer

I see, okay.

00:12:43 TPR2

So, mainly these three types.

00:12:46 Interviewer

So, let's move on to the second question. What do you think is the main target of cyber attacks in Taiwan right now, and what are the reasons?

00:12:58 TPR2

As for the target, it depends on the industry. Each industry is different.

00:13:03 Interviewer

It's okay, you can just give us a general idea of what you know.

00:13:10 TPR2:

For example, banks. Banks transfer money, so their target is definitely their transaction software, Swift. Banks exchange with each other through Swift, and that's their target. So,…. Do you know about the Far Eastern International Bank? You might not have heard about it, it's a bit old news.

00:13:43 TPR2

The case of Far Eastern International Bank.

00:13:47 Interviewer

No, I don’t know.

00:13:47 TPR2

You were probably still in high school.

00:13:50 Interviewer

No, I don’t know.

00:13:50 TPR2

Just, compared to before, they will go inside, then try to do transactions like transferring money. They must go into Swift to create fake tickets and maybe say, 'Today I want to transfer to someone, someone, someone. Please approve it.' They use fake tickets, and their goal is to transfer money through Swift. Like you see in Mumbai, right? Or some similar methods. They target the banks to attack Swift. However, recently, Taiwan's security has improved, so there are fewer incidents like this. In the manufacturing industry, their target might be SAP, right? SAP or SEP, I forgot, their mainframe. Inside, they will have transaction data or some confidential information, and their target might be what they put on their NAS (Network Attached Storage). That's what they are after.

00:14:38 Interviewer:

I see.

00:14:40 TPR2

For example, some of our suppliers have a close relationship with Apple and other large US companies. Some of the design blueprints, IT industry designs, and confidential information are stored on servers in Taiwan, and these are also targets for theft and extortion by those who have obtained them and are trying to extort US companies, right? So, the targets will vary depending on the industry.

00:15:12 Interviewer

I see. In that case, where do you think attacks are more likely to occur in certain industries?

00:15:20 TPR2

Um, the main reason why some industries are more vulnerable to attacks than others are because it depends on how much importance they place on cybersecurity. Currently in Taiwan, only banks are serious about cybersecurity. Other industries are not as focused on it.

00:15:40 Interviewer:

Is the awareness not that high yet?

00:15:45 TPR2:

Yeah, they just shrug their shoulders and say 'I don't have any important information for you to steal.' That's why they don't take any precautions because they think that good cybersecurity is expensive. In Taiwan, people feel that their data is not that valuable.

00:15:59 TPR2:

So they don't really do anything about it. The main target of attacks depends on whether the industry takes cybersecurity seriously or not. In Taiwan, we saw some problems with banks a few years ago, but in recent years, we haven't seen any issues with banks. Other industries are starting to take notice now.

00:16:14 Interviewer

I see. So, banks are doing well in terms of cybersecurity?

00:16:17 TPR2

Because it's required by regulations, and Taiwan's, all our cybersecurity regulations start from the banks, so the banks are doing relatively well. But our manufacturing industry in Taiwan is vast, and besides what you see in the news like TSMC (Taiwan Semiconductor Manufacturing Company) doing well, others are... Of course, there have been improvements, but they haven't been very rapid, and it still needs some time, right.

00:16:44 Interviewer

I see. So, let’s move on to question 3. What do you think are the reasons that impact the overall cybersecurity in Taiwan?

00:16:59 TPR2

Um, the reason.

00:17:00 Interviewer

Right, the factors.

00:17:01 TPR2

In fact, the factor is that Taiwan's cybersecurity awareness is not that good. It's like, it's like when it comes to cybersecurity, people feel the same way as driving. Taiwanese people, whenever they drive, it's like driving is very popular, and it's like, whoever collides with whoever, oh you were not in Taiwan, right? So, you just don't know.

00:17:26 Interviewer

Are you talking about this year? I was in the UK only in the past year, um, right, right, right.

00:17:32 TPR2

Ah, because in Taiwan, this month, there have been many car accident incidents, and they have been reported in a chaotic manner. And, for driving in Taiwan, you can't really say, 'I want to regulate how you drive,' that's very difficult. You might just say, 'Oh, how you drive on this road,' but it's impossible to regulate how someone drives. So, you must have your own awareness, like I shouldn't drive like this. Similarly, Taiwanese people and Taiwan's cybersecurity are the same. Currently, there is no awareness of how to do things securely. None at all. So, in this regard, the cybersecurity awareness is not good enough.

00:18:13 Interviewer

Mm-hmm.

00:18:13 TPR2

Yes, that's right. So, I think Taiwan's awareness is not there yet, it hasn't risen. It may need some more time for them to realize that, "Hey, this is something I need to protect, so I should invest resources to do it." This year might be slightly better, as larger industries might start implementing cybersecurity measures, but small and medium-sized enterprises are still lagging behind, yes, yes, yes.

00:18:39 Interviewer

Mm-hmm, so it's mainly about people's awareness?

00:18:44 TPR2

Yes, people's awareness is important, and there should also be an awareness from the bosses, such as the operations director of a company, whether they really value this or not, there is a difference.

00:18:58 Interviewer

Hmm, so decision-makers themselves need to value it?

00:19:02 TPR2

Yes, but even if the lower levels have it, they are still young and although they have this cybersecurity awareness, they cannot change the fact that there is no awareness at the top. They may propose something, saying, "Oh, we need to purchase this," but the executives say, "Oh, we don't need this," and it gets dismissed or becomes useless. So, as you mentioned earlier, the awareness of the decision-makers is the most crucial.

00:19:20 Interviewer

Okay, got it.

00:19:24 Interviewer

Then, I want to ask again, do you think that in addition to the awareness you just mentioned, there are any political factors in internet security issues in Taiwan, such as stealing commercial secrets for political gain, or for commercial interests or political reasons?

00:19:49 TPR2

Well, for politics...

00:19:52 Interviewer

Or is it more that you haven't come across them much? Political factors may involve things like cyber armies.

00:19:53 TPR2

We have less contact with politics.

00:19:57 TPR2

If, well, in terms of politics, there could be the possibility of political cyber warfare, which involves data theft. If you want to talk about why Taiwan is not doing well in terms of cybersecurity, another reason is that the penalties for cybersecurity issues in Taiwan are relatively light. When a breach occurs, it may be treated casually, and there are not significant penalties. It's similar to how we handle environmental issues; heavy pollution is a serious matter, but the penalties are light, like a fine of 300,000 NTD, which doesn't create much impact. You know what I mean? The cybersecurity regulations and government standards are not well-established, leading to a lack of emphasis on cybersecurity, which could be a possible reason.

00:20:49 Interviewer

I see, got it.

## Section F

00:20:57 Interviewer

So now let's move on to the section F. The F part is about some issues related to the defense strategy of network attacks. The first question I want to ask is what kind of technical services do you provide to customers in terms of network security? You probably mentioned it just now.

00:21:18 TPR2

As for technical services, it mainly involves the investigation part. For example, we go to the customer's side, and it can be divided into two parts. One is the investigation part I just mentioned, and the other is the part where we monitor the customer after the investigation is completed. These two are both more technical aspects. One is investigation, and the other is monitoring. These two, well, are not directly related, but they are services that can be provided in a sequential manner. Customers don't have to choose both of the services. That’s fine if you only want to choose our latter service without the former one. So we mainly provide customers with IR, which is incident investigation services and monitoring services. These two are the main services we provide.

00:22:11 Interviewer

I see.

00:22:13 Interviewer

The second question is about your main customers.

00:22:16 TPR2

Our customers are from all over Taiwan, and there is no specific limitation.

00:22:19 Interviewer

Are they mostly enterprises or are there others as well?

00:22:24 TPR2

Oh, our department is mainly focused on enterprises because we also have another customer department that deals with general marketing, and normal users also buy our antivirus software.

00:22:38 Interviewer

Oh, so even individual users use your software?

00:22:40 TPR2

Yes, that's another department. My department mostly deals with enterprises, and there is no distinction between large, medium, and small ones. We have customers of all sizes.

00:22:54 Interviewer

In that case, when these enterprises purchase from you, do you provide them with software or is it like what you just mentioned, where you conduct testing and investigations, provide a report, and then suggest how they can improve? Do you sell them some software as well, or is that handled by another department?

00:23:20 TPR2

Yes, another department. Our department mainly focuses on, because we are the IR department, the IR team.

00:23:26 TPR2

So, there are other departments like sales, support, and possibly many other departments, each responsible for their respective business areas. In comparison, our department is solely focused on providing cybersecurity technology solutions, and software is not our responsibility. However, they (customers) still use our products because [a private company] itself produces products, and they also use our products.

00:23:51 Interviewer

Hmm, what do you usually do if they (customers) don't use your products?

00:23:56 TPR2

This can be divided into two parts. If they are not using our product, then the monitoring aspect won't be applicable, as our main focus is on using our product for monitoring. However, in the first part, most of the cases involve customers who originally used other vendors' antivirus software or other products. But when they encounter incidents, they might have been hacked and possibly subjected to ransomware attacks.

00:24:25 Interviewer

I see, I see.

00:24:26 TPR2

Usually, because they buy products from foreign or other international vendors, they may not have strong capabilities in incident investigation. In fact, when it comes to incident response planning, [a private company] is considered a leader in Taiwan and probably no one would say it's second. So, basically, they would come to us to help them investigate what happened, why they were breached, and then we would send a team to conduct the investigation.

00:24:58 TPR2

So, my customer source may come from the fact that they are not used to be our customers, but they need to investigate because something happened. Then they will look for people in Taiwan who provide this service to help them, so our customer source will be established in this way.

00:25:16 Interviewer

OK, I understand.

00:25:19 Interviewer

So, for the third question. As I mentioned earlier, the main reason why the customer seeks your service is because they may have been invaded or their anti-virus software has experienced some issues, and they need someone to investigate. Later, they may end up using your software so that you can provide a more comprehensive service.

00:25:52 TPR2

Yes, for the most part, they may feel that it's possible, as I mentioned earlier regarding consulting services. Currently, only we, [a private company] provides more of such services . Most of the time it's probably because they want to improve their environment and they hope to find someone to help them with that. They usually turn to KPMG, which is like... Deloitte & Touche, right?

00:26:18 Interviewer

Deloitte & Touche?

00:26:19 TPR2

This is onecthat should be considered as Taiwan or foreign, I forgot, but they are also doing, oh, foreign, is it called Deloitte? Have you heard of Deloitte? They specialize in consulting, for example, auditing your environment to see if it is secure enough, and some may approach them. However, some people might find them not practical enough and come to us. But this doesn't necessarily mean that something has happened. They may just want to enhance their company's security level and then also approach us.

00:26:48 Interviewer

Hmm, so the one you just mentioned, like KPMG, is that a government-provided service? Or are they also private?

00:27:01 TPR2

They are private, but what they provide is more like a document-based interview. For example, they will have many documents stating what regulations you need to comply with, what you need to do, and after you meet certain requirements, then it will be considered completed. This approach is more standardized, and they cannot provide a more customized view or advice on your specific environment. So, they offer fewer customization options, whereas we specialize in providing more customized solutions.

00:27:32 Interviewer

Okay, got it.

00:27:35 Interviewer

So let's move on to the fourth question. Based on your experience working with your clients, which areas of their cybersecurity do you think are generally lacking?

00:27:51 Interviewer

And where do they need help in terms of planning?

00:27:51 TPR2

They're lacking in pretty much every area.

00:27:55 Interviewer

Overall, you mean?

00:27:55 TPR2

Yeah, overall. It depends on the size of the client, though. For most medium-sized businesses in Taiwan, they are lacking in a lot of areas.

00:28:08 Interviewer

Medium-sized businesses?

00:28:10 TPR2

Yeah, medium-sized businesses in Taiwan. What we consider to be medium-sized businesses here might be small businesses in other countries. For many of our medium-sized clients, they are lacking in most areas.

00:28:24 TPR2

For large enterprises, their strength lies more in perimeter defense. Perimeter defense refers to protecting the enterprise when it is globally distributed. It includes safeguarding from external threats that can come from websites, emails, or any connections from the outside into the internal network. All these aspects are considered part of perimeter defense services.

00:28:44 Interviewer

I see.

00:28:49 TPR2

For larger enterprises, their understanding and implementation of perimeter services tend to be better, but even after the perimeter services have been breached, their internal security may not be as robust. Because there are different defensive measures for the internal and external aspects. In the past, most companies emphasized defense against external threats while not paying as much attention to internal security. However, in recent years, there has been a shift in focus, and internal security has become more important. Because there are so many attacks from the outside, it's impossible to defend against all of them. There will inevitably be times when some attacks get through. That's why you need to focus on strengthening your internal defense, controlling its impact, and figuring out how to monitor it. There's quite a lot to do in this regard.

00:29:31 TPR2

But if we insist on talking about it, in Taiwan, we may not emphasize the internal aspects as much, especially in large enterprises.

00:29:40 Interviewer

So, in this case, your department provides sufficient internal defense measures, right?

00:29:50 TPR2

Yes, internal network detection and defense, that's right.

00:29:54 Interviewer

So, this can be in response to our sixth question. This is about how to reduce damage, for example, after the perimeter services are breached, how do you effectively defend in terms of incident management?

00:30:20 TPR2

When, um, when your environment is compromised, you need to first confirm the attack method, where it came from, because this is a top priority. Since the intruder has just entered your environment, you must know where they came from and cut off that entry point first. After cutting it off, then you can see where they can go once they are inside.

00:30:48 TPR2

For example, because you should have a basic understanding of networks, right? Network fundamentals, like how to set up an internal network. If you haven't implemented any defenses, then it's possible for anyone to connect everywhere. For instance, let's say I'm using computer A, and your computer is located elsewhere. If I find your IP address, I can connect to your computer. In terms of cybersecurity, this shouldn't be allowed. If we are in different departments, we shouldn't be able to connect directly like that. This is what we call damage control. After my computer gets compromised, I should at least prevent the hacker from accessing your department, limiting the impact to just my own department.

00:31:39 Interviewer

Hmm, wouldn't it affect anyone else, right?

00:31:40 TPR2

Yes, it won't affect others, this is what we call damage control. So, after we know how they got in, we cut off that entry point first. Then we can see where they can go once they are inside your computer. We need to identify their targets and where they jump to from the computer. We gather all this information and then check the other computers they might have visited. After examining them, we will know their objectives and destinations. Once we have all the information, we can start taking actions, such as taking the compromised machines offline and blocking their access points. This is the damage control part.

00:32:17 Interviewer

OK.

00:32:18 TPR2

As for incident management, it's more like the defensive measures we need to take. It's not something we do when an incident occurs.

00:32:34 Interviewer

Incident management. It means there will be many incidents that need to be handled and managed. It is more about handling and managing after incidents occur.

00:32:49 TPR2

Okay, this may need to be translated as reducing damage and recovery, reducing damage. Because incident management is a bit of about what we manage. I think we should translate it into accidents instead of incidents, yes, reducing accidents.

00:33:26 TPR2

Okay, okay, good.

00:33:30 TPR2

It should be translated as how to reduce...how to reduce the occurrence of cybersecurity accidents...when cybersecurity accidents occur, how to reduce their damage and scope of impact? That should be it, because incident management is a bit like, when the environment is still secure, and you have some things that need to be collected, such as login records need to be collected, what are the management methods after collecting them? This may be a bit different.

00:34:14 Interviewer

You said that would be more like defense?

00:34:18 TPR2

It's what you do in defense, that is, when your environment has not yet experienced an incident, but you must collect all the records of logging in and out of each computer. When you have an accident, you can use these records to investigate the source of the intrusion. It's like some practices before the incident is discovered, but it looks like the translation should mean what to do when the incident occurs? That's right.

00:34:51 Interviewer

Right, right, it's probably right.

00:34:54 TPR2

If we talk about what actions to take, as mentioned earlier, we will inform you about the scope of the impact and what measures you should implement, such as purchasing certain products for defense. We will also analyze the attacker's methods in the second intrusion. For example, did they use RDP to gain access everywhere, or did they employ a network neighbor attack, or perhaps they exploited vulnerabilities? These conclusions are based on the investigation, and then we will propose corresponding measures for you.

00:35:20 Interviewer

Mhmm.

00:35:22 TPR2

Yes, it still depends on what happened.

00:35:24 Interviewer

Okay.

00:35:25 Interviewer

Okay, then this may also connect to the seventh question, which asks about your company's cyber resilience in providing technical services.

00:35:38 TPR2

Actually, we don't provide restoration services. Resilience, you mean cyber resilience?

00:35:44 Interviewer

Yes, cyber resilience is like having backup plans in case of an incident. For example, when there is a sudden power outage, you have some reserve power to supply to prevent the entire company from being shut down. This is the concept of resilience. But now we are talking about cyber resilience.

00:36:13 Interviewer

So, after your network was attacked?

00:36:16 TPR2

Well, we should call it, well, more like we are not currently offering a restoration service. For example, if your database gets compromised and encrypted, and you need to restore them. But, we don't have the necessary product for data restoration because it requires purchasing specific products, which we don't offer. However, we can provide recommendations on what you should do when facing such situations. For instance, we can suggest buying a backup server and implementing off-site data redundancy. We can guide you on how to set up two locations for backup and how frequently the backup should be performed. While we can offer advice on these matters, the actual implementation is done by other vendors, as we do not provide this service ourselves.

00:37:26 Interviewer

OK, I understand now.

00:37:29 Interviewer

So, you basically help plan and give them some advice, and then OK, let them do it.

00:37:36 TPR2

Then, they should find other vendors to do it because our company doesn't cover everything.

00:37:39 Interviewer

OK, I see. Let's go back to the fifth question, which is about the types of network attacks that your clients mainly face.

00:37:52 TPR2

The types, network attack types?

00:37:55 Interviewer

Like what you just mentioned, maybe it's ransomware, or something else.

00:37:59 TPR2

Yes, exactly. We handle various tasks. Mostly, if it's related to networks and not physical equipment, we take care of it.

00:38:11 TPR2

We handle everything. What are the main attacks that we handle?

00:38:15 Interviewer

Right.

00:38:17 TPR2

Currently, since 2020 and based on last year, ransomware is still the most common.

00:38:30 TPR2

The second most common type is probably China's internet army.

00:38:37 TPR2

Yes, these two are the main types. Because there is money to be made, everyone will come to attack. The third type is probably stealing your personal information and selling it. It happens.

00:38:50 Interviewer

OK.

00:38:51 TPR2

Yes, for example, recently in Taiwan, there was a data breach where personal information of many people was sold, right? One of the incidents involved data being leaked, and it might be related to China.

00:39:04 Interviewer

So in that case, let's jump to question eight, since we already asked about six and seven earlier.

00:39:16 Interviewer

This one may be a bit sensitive, but basically, since nothing is perfect, questions eight and nine can be answered together, are there any areas in the services your company provides that you think could be improved upon in the future, and how could they be improved upon?

00:39:37 TPR2

For our company, we mainly provide technical services... anything lacking?

00:39:51 Interviewer

Or anything that could be done better, maybe in an area that hasn't been fully developed yet, but you have plans to improve in the future?

00:40:01 TPR2

There are many complaints every day, does that count?

00:40:05 TPR2

I think currently, it's not really a technical service issue, but rather a problem with the structure.

00:40:16 Interviewer

A problem with the structure?

00:40:17 TPR2

It's not exactly a technical issue. If we're talking about technical issues, we only talk about our department, right? For our department, from a technical standpoint, there shouldn't be any deficiencies. However, the only possible inadequacy is probably the shortage of personnel.

00:40:37 Interviewer

The shortage of personnel.

00:40:38 TPR2

Because our technology is considered quite advanced, yes, they are quite advanced, right. I think it should be because, well, we are all very technical people, so maybe in terms of documentation, we may not be as thorough as other vendors.

00:40:50 Interviewer

In terms of documentation?

00:40:56 TPR2

In terms of documentation, it's about document management. For example, if we want to type our something like this, we are not able to do it. It's probably like this it. it's because we may lack comprehensive documentation. Yes, we are unable to record everything in detail, but this is not related to technical aspects; it's more about documentation and management.

00:41:17 Interviewer

So that means in certain areas, such as in terms of information security, your professional technical skills are very professional, but in addition to providing these professional technical skills, as you mentioned, you may still need to provide reports to customers that they can understand. You need to use their language to let them know what you are talking about.

00:41:34 TPR2

Yes, yes, yes, something similar to that. If we were to compare with other vendors, it's true that our documentation may not be as elaborate, not written as beautifully. Some consulting service providers are very thorough in their documentation, and each item is explained very well. However, we don't have that kind of expertise because our background is technical, and we don't have dedicated writers.

00:42:01 Interviewer

OK.

00:42:04 TPR2

Yes, so I think it's the document part.

00:42:05 Interviewer

So, is it related to the structure or the lack of personnel, or what else?

00:42:12 TPR2

Yes, yes, that's right.

00:42:15 TPR2

Technical services, well, as I mentioned earlier, we hope to improve our documentation and system to fill in the gaps. In our technical services, many aspects require automation or documentation, which we currently lack in terms of completeness. So, we need improvements in this area. Our services also lack consistency. For example, if I provide a service and you provide a service, there might be different results. When offering services, we need to maintain consistency and ensure that the quality doesn't vary too much. Achieving this will involve several aspects, such as automation, communication, and standardization.

00:43:07 TPR2

For this part, we don't put much emphasis on it. As long as we can recover afterward, it's fine, and the customers can understand that. As long as there are no customer complaints, there won't be any issues. That's where we are lacking, yes, we are lacking in that area.

00:43:22 Interviewer

But do you still think that standardization is necessary?

00:43:26 TPR2

Yes, it is necessary. It's a must.

00:43:27 Interviewer

Hmm, so that it can be passed down in the future, right?

00:43:30 TPR2

Yes, the more people there are, the more chaotic it will be due to different methods used. It must be done. We are currently doing it and should do it better this year.

00:43:42 Interviewer

OK.

00:43:43 Interviewer

So, this also answers the 10th question. You mentioned earlier that the company plans to make improvements in this area this year, right?

00:43:54 TPR2

Oh, only our department. Our company is too vague, and I'm just a engineer in a small part of it, you know.

00:43:57 Interviewer

Oh, it's okay. In terms of your department, just answer with regards to the aspect that your department intends to improve.

00:44:05 TPR2

Similarly, it's about documentation, technical documents. In fact, we all do our own research. For example, if I study something and understand it, teaching others can be a bit challenging. You can explain it verbally, but then you may wonder if there are any references or resources for them to look up. No, you have to Google it by yourself, it ends up like that. There's not much available to quickly bring others up to speed. So, perhaps documentation and as I mentioned earlier, providing services with consistency, that's the main issue, and also the automation of systems might not be sufficient.

00:44:45 Interviewer

Automation in the system?

00:44:46 TPR2

Yeah, because with more clients, there's not enough personnel to keep up with the demand. So, automation is needed to improve the problem of personnel shortages, like factory automation.

00:44:58 Interviewer

Okay, got it.

## Section G

00:45:03 Interviewer

Okay, then let's move on to section G, which is about the collaboration between public institutions and private companies like yours.

00:45:17 Interviewer

And, okay, let me explain first. In this aspect, from what I understand, I also know that, well, companies like yours, as technology or service providers, have relatively limited collaboration with public institutions at the moment.

00:45:40 Interviewer

Yes, it's relatively lacking in this kind of experience. And I mean, not just in Taiwan, but also in other countries. However, many countries actually highly promote collaboration between public and private sectors. For example, government agencies may have the power and authority but struggle to attract top talents, who often end up in companies like yours. So, they really need your expertise. That's why I wanted to explore this topic and see how we can potentially collaborate in the future. So, there are no right or wrong answers to these questions; you can answer based on your own perspective. That's all.

00:46:23 TPR2

Is this your topic? Oh, I didn't read the title.

00:46:29 Interviewer

Yes, that's okay. So, let's move on to the first question.

00:46:37 Interviewer

The question is, in your opinion, what do you think about the collaboration between public and private sectors in terms of network security?

00:46:50 TPR2

Actually, we have collaborated quite a lot.

00:46:52 Interviewer

Really? Oh, that's great.

00:46:54 TPR2

Our approach is basically, well, you just mentioned the National Police Agency, MOI earlier, right? Is your senior ( refer to someone who is older or more experienced back in the school ) from the National Police Agency, MOI?

00:47:02 Interviewer

No, not just National Police Agency, there are many that have, also have the National Police Agency, but yes yes yes.

00:47:09 TPR2

Our approach is that we work with the Criminal Investigation Bureau and the National Security Bureau.

00:47:17 Interviewer

Hmm, okay, so you cooperate with them?

00:47:18 TPR2

This should be, let me think, because there will be recording, actually we, um, the National Security Bureau, Criminal Investigation Bureau, and the Ninth Investigation Division, they all have cooperated with us, and they, actually, most of the problem is, as you just mentioned, they have public authority, but they are not very familiar with the technical aspect because their personnel may keep changing, and they may not be very specialized in cybersecurity or investigative work, right, but they still need to do something, they need to have some achievements or results, so they actually come to us and say, for certain companies, when they need to be audited or when they need to do something, we can go along, um, of course, we go as their personnel to do these things, right, right, so this time it's kind of like a private collaboration between the public and private sectors, but..

00:48:26 Interviewer

So it's not publicized, right?

00:48:30 TPR2

No, it's not publicized.

00:48:31 TPR2

Okay, this seems to be not very public, not very sure, but there will be some collaboration on certain things.

00:48:36 TPR2

Um, yeah, in terms of cooperation, it is beneficial for both the public and private sectors.

00:48:43 TPR2

For example, they, they may receive a real-time report that a certain unit has a problem, and they need to investigate. When they feel that their investigation capabilities are insufficient, they come to us. After we go, we will help them with certain tasks, and then they will write the report. We provide them with the data and let them take it from there, let them do the rest.

00:49:03 Interviewer

Hmm.

00:49:10 TPR2

This time we help them, and next time, assuming we need some means, they will help us. For example, when we are working on many cybersecurity matters, there may be some relays or relay stations involved. If these relay stations are in Taiwan, for instance, they could be in a certain data center of Chunghwa Telecom or a private telecom company, and they have already been invaded and used as relay stations. Then we can ask them, 'Hey, can you help us take them back?

00:49:41 TPR2

Then they will use their authority and talk to the personnel at their data center, saying that they need to take away a particular machine and request their cooperation. They will then hand it over to us, allowing us to conduct deeper research and investigation. So, it can be considered as a more discreet form of cooperation. This is one of the examples; of course, there are others, such as collaborating with the Criminal Investigation Bureau or some other unit, privately.

00:50:08 Interviewer

Hmm, so it's all relatively private at the moment?

00:50:12 TPR2

Yes, this collaboration actually has its benefits, because, um, there are several advantages. They can let those industries know that these things are very important, and it can also allow our companies in Taiwan to obtain more information and verify if there are other victims. After we collect this intelligence, we will examine all our customers to see who has been affected, especially by the same batch of people who use the same relay stations.

00:50:49 TPR2

Then, after we retrieve the data, we can start to check all our customers to see which ones have been compromised. If any of them have been compromised, I will notify them and say, 'Hey, you have been hacked. Do you want to take action?' Because most of them are unaware of it.

00:51:00 TPR2

So, this kind of more private cooperation actually helps our company identify those who are unaware of being hacked. It is indeed helpful.

00:51:12 Interviewer

So you mean, it's helpful for your own company, and for the people, and for their law enforcement agencies?

00:51:19 TPR2

Yes, and it seems that I’ve covered question one and three.

00:51:22 Interviewer

Yes, that's right. So, I want to ask again, for example, the second question. In Taiwan, the cooperation currently seems to be more private and there isn't a well-established, standardized mode of collaboration, right? It's more like if there is a need for assistance, then you are asked to help, right?

00:51:46 TPR2

If there is, then they have also asked us to provide education and training. It's like we conduct some courses, but these courses are not open to the public.

00:51:59 Interviewer

Are you teaching their internal personnel?

00:52:00 TPR2

Yes, that's right. It's about some contractual matters. So, I would say, "Oh, today we invite you to our Criminal Investigation Bureau to attend the class and teach them some investigation tools and how to examine these records. We conduct the training to let them listen and learn.

00:52:20 TPR2

The more formal collaborations are of this kind, and also, yes, mostly they are visible. The majority of these visible collaborations are related to education and training, with educational training sessions being the most common. As for other types of collaborations, they are not as prominent or publicly visible.

00:52:40 Interviewer

So what do you think about the current methods of cooperation? Do you think they're sufficient? Is there anything that could be developed to make things better?

00:52:52 TPR2

Well, for the public sector, I think they should come up with more complete laws or frameworks for overall cybersecurity, so that companies in Taiwan or the public can follow these regulations or guidelines.

00:53:23 TPR2

To ensure that everyone's foundation is the same, and there won't be some who completely lack it. The scariest thing we've seen is some e-commerce companies, their databases are just placed beside a warehouse, and they start doing business without any firewalls in front. This is something that……placed in iRent or someting?

00:53:47 TPR2

iRent, didn't they have a data leak incident recently? Right, many of small and medium-sized enterprises are like this, it's just a matter of whether or not it's reported.

00:53:54 Interviewer

Yes, yesterday the police officer I interviewed mentioned this incident to me.

00:54:00 TPR2

Ah, yes, that's a very basic cybersecurity issue. I'm not sure if it was accidental or deliberately left unprotected. But this kind of thing should not happen. Especially when it comes to exposing sensitive data to the outside world. Each company's level of cybersecurity knowledge varies, and that's why the government should establish clear regulations and standards. They need to make sure companies understand the required level of cybersecurity before they can conduct their business. Some countries prioritize cybersecurity, and they don't overlook such important matters. It's a fundamental concept.

00:54:44 Interviewer

Just like human rights, so that's why I need to deal with all these things.

00:54:48 TPR2

Right, you must have the basics, and then you can build your business on top of it.

00:54:54 Interviewer

OK, so do you currently feel that, based on your understanding, that in the future, is there a direction that this collaboration is heading towards? Have you heard anything about it?

00:55:14 Interviewer

If you work with law enforcement agencies, have they mentioned that they may need to contact you in the future to do something?

00:55:24 TPR2

Oh, this is more of a business matter. For the most part, after our business department negotiate some things with the government, we will help them with technical assistance. I don't think this falls under the scope of the IR team.

00:55:43 Interviewer

OK, I understand it's a business matter.

00:55:44 TPR2

Yes, it's a business matter. However, there are some things we do privately, which cannot be improved because they are done privately. This is also more of a business aspect.

00:56:00 Interviewer

I understand. So, you have collaborated with law enforcement agencies before, such as the National Police Agency?

00:56:07 TPR2

Yes, but not just them. Almost all the units in Taiwan.

00:56:11 Interviewer

Taiwan’s Ninth Investigation Division? Or the National Security Bureau

00:56:13 TPR2

Yes, yes, yes, those actually exist, it's just a matter of how widespread or whether there's a formal contract or not. Those without formal contracts will still happen, yes.

00:56:21 Interviewer

OK, I see.

00:56:23 Interviewer

So, I think that will be all for this interview.

00:56:28 Interviewer

Thank you for providing us with a lot of information.

00:56:33 TPR2

Oh, it's nothing. It's just that I am...