# Transcript

## Section A

00:00:00 Interviewer

Next, we will conduct an interview with TPR6 from [a private company].

00:00:05 Interviewer

Let's start with question A. Since you are from a private network security provider, we don't need to ask about that. The second question is, what company are you currently working at?

00:00:18 TPR6

[A private company].

00:00:19 Interviewer

What department do you work in?

00:00:21 TPR6

The Sales Department.

00:00:23 Interviewer

How long have you been working there?

00:00:26 TPR6

Four years.

00:00:28 Interviewer

Four years, and what is your current position?

00:00:31 TPR6

Deputy Sales Manager.

00:00:34 Interviewer

Wow, impressive.

00:00:36 Interviewer

So, what are your main responsibilities?

00:00:39 TPR6

To sell and promote the company's information security equipment, and to provide customers with solutions.

00:00:45 Interviewer

OK, so you mainly provide both hardware and software?

00:00:49 TPR6

Hardware, mainly. The hardware is integrated with software that has the device's functions, which can generate solutions.

00:01:02 Interviewer

Just confirming that the recording is on.

00:01:07 Interviewer

Next, let's proceed.

## Section E

00:01:10 Interviewer

We've finished part A, and now we're moving on to part E.

00:01:15 Interviewer

Part E has three questions, and it's about internet security. So, for the first question, based on your experience, what do you think are the main internet attacks that Taiwan is facing? What are the attack methods, and can you give an example?

00:01:34 TPR6

Well, there are many methods of internet attacks. For example, there are ransomware, Trojan horses, worms, and so on.

00:01:43 Interviewer

What else?

00:01:44 TPR6

Worms and worm viruses, yes.

00:01:47 TPR6

Actually, these things are all important ways to invade internal organizations. After that, the attacker may use various methods to paralyze the network. For example, they might start by scanning ports, and then there's also control.

00:01:58 Interviewer

Doing what?

00:01:59 TPR6

Scanning ports. Some of our open services have ports.

00:02:04 Interviewer

I see.

00:02:06 TPR6

For example, the 443 port is a network service port, and the 80 port is a web service port. Some are encrypted connections, while others are unencrypted connections.

00:02:12 TPR6

So, the attacker may see some ports that are vulnerable and use them to invade. Then, once they invade, they'll want to control the computers inside to do bad things. After controlling the computers, they may form a series of zombie networks, because the internal computers may not be protected, and one infected computer may infect another, and so on. All computers are connected as a zombie network. So, this is why the attacker can paralyze many devices, and we often hear news about devices being paralyzed and unable to operate because of this.

00:02:45 Interviewer

I see.

00:02:47 TPR6

There is also a phishing email that is like social engineering.

00:02:51 TPR6

There are actually many types of social engineering, such as email, text messaging, LINE, or even something like a USB drive you might see on the ground. Social engineering is when something around me that is closely related to me sparks my interest and leads me to click on a link, input personal information, or open an attachment. For our company, we mainly focus on email social engineering. Essentially, it is about luring people to click on a link and input their personal information. After obtaining someone's personal information, a hacker can implant a Trojan horse program and use it to spy on the company’s data and engage in extortion when someone clicks on a link like this.

00:03:40 Interviewer

Okay, then let's move on to the second question, which is what are the main targets of cyberattacks in Taiwan and why?

00:03:55 TPR6

For the main targets, I think it can be divided into academic networks and large organizations and enterprises, such as famous institutions. The reasons vary. And there are also some public service units, for example, those related to oil, water, and electricity, such as CPC Corporation, Taiwan Water Corporation, Taiwan Power Company, etc. For academic networks, students' learning files are very important, so hackers might encrypt these files and extort some institutions by exposing them to the public. It may become a news headline. Another example is the well-known event involving TSMC. This falls under the category of enterprises. TSMC and Gigabyte were both targeted by hackers before.

00:04:02 Interviewer

I know about the Gigabyte incident involving industrial computers.

00:04:24 TPR6

Yes, that's right. And then there are those like the PCB manufacturers, which have some design plans that can be encrypted, and then through ransom demands, if you don't agree, they can gradually release your important design plans. Such as the design plans you sell to Apple today, or your personal information, salary, the salary of senior executives, and other important information that may gradually leak out. This is why hackers would want to attack these important units.

00:05:20 Interviewer

So what you just mentioned are TSMC and Gigabyte.

00:05:23 TPR6

Yes, and also the PCB manufacturers.

00:05:24 Interviewer

PCB.

00:05:28 Interviewer

That's it.

00:05:29 TPR6

Um, I remember what it's called, um?

00:05:31 Interviewer

Is it also a company?

00:05:32 TPR6

Yes, it's a company that produces PCBs, and it's very famous, listed and over-the-counter (OTC).

00:05:39 TPR6

They will definitely be attacked today, as they are well-known companies. In order to create a sensation, to let everyone know that they have been blackmailed and their things have been controlled, hackers are also people, so they hope to get their money, so they will look for some important units. For example, in the previous Pelosi incident, they would attack some civilian boards, and when Pelosi came, our attack frequency soared, hmm…the network attack part increased. So this is why, with news comes traffic, and with traffic people will pay attention, and the Internet is actually closely related to people.

00:06:14 Interviewer

So, my third question is, what do you think are the factors that affect Taiwan's internet security? Can you give an example?

00:06:24 TPR6

The factors that affect Taiwan's internet security, I think the first one is...

00:06:30 TPR6

Oh, wait, let me clarify first. Do you want to understand the relationship that affects Taiwan's internet security? In other words, what actions can cause the impact of Taiwan's internet security to become better or worse?

00:06:49 Interviewer

Yes, that's right. Whether it gets better or worse.

00:06:55 TPR6

The relationship that affects the internet is a very broad topic. One part is related to the development of technology. For example, we use more and more applications, such as TikTok and Xiaohongshu, many of which come from China. Are there any security concerns with these things? To be honest, there may be, so sometimes we need to do application control in our firewall. For example, in government agencies, they are not allowed to use apps from China, etc., and this also affects the internet. Next is about our cybersecurity awareness, whether everyone's cybersecurity awareness has been improved. From my perspective, I even have a tendency to click on links from unknown sources and easily open images. When I click on such an email, there's a high possibility that I might be infected with a bot, which could already be implanted on my computer.

00:07:47 TPR6

In this aspect, it also relates to the impact of the internet. Furthermore, it means that today, I might not have taken proper measures, such as controlling external-to-internal traffic, or I might not have any firewall within the company. Instead, I could simply be using an IP router, like the one provided by Chunghwa Telecom, to connect to the internet.

00:08:10 TPR6

And I have not done any data protection or backups. Actually, this part of internet security is quite worrying.

00:08:22 Interviewer

Right, so what you said earlier, the first thing you mentioned, was like, um, kind of like political factors?

00:08:30 TPR6

Um, are you talking about the news part?

00:08:32 Interviewer

I mean, like what you said about using apps like TikTok and Xiaohongshu.

00:08:34 TPR6

Ah, political factors. For example, the recent war between Russia and Ukraine. Actually, for us, as a security company, our antivirus software includes Kaspersky. But during that period, Kaspersky was boycotted because of the political situation.

00:08:51 Interviewer

What is Kaspersky?

00:08:52 TPR6

It's a Russian antivirus software. It's actually related to politics. At that time, people tended to use antivirus software related to the US.

00:09:05

Hmm, I see.

00:09:07 Interviewer

Okay, and the second thing you mentioned was like people's awareness?

00:09:09 TPR6

People's awareness. In fact, many cybersecurity issues on the Internet are caused by people themselves touching things they shouldn't touch.

## Section F

00:09:19 Interviewer

Alright, let's move on to the section about F, which is about network attack defense issues. So, the first question I want to ask is about network security, and what kind of technology or services your company provides to customers?

00:09:38 TPR6

Well, first of all, we would probably take inventory of their network architecture environment and see which part needs to be reinforced. We may conduct a vulnerability scanning of the host, do a vulnerability scanning of the website, and then look at all the cybersecurity vulnerabilities based on the low, medium, and high risks identified through the vulnerability scanning, and then suggest areas for improvement, such as regularly updating firmware and upgrading networks.

00:10:06 TPR6

Next, we would examine their firewall connections. If they don't have a firewall or other cybersecurity protections, we would recommend that they implement them.

00:10:14 TPR6

This includes things like separating the external network from the internal network. For example, if they have an office side and a production side, these network segments should be isolated. It shouldn't be just one closed, all-in-one internal network environment. In terms of email, we provide email cybersecurity protection.

00:10:31 TPR6

Because sometimes the email server is on their end. I would need to do some email filtering, detect phishing emails, and detect email firewall breaches. As for the rise of people's awareness, we would conduct social engineering exercises, and regularly provide them with education and training. After the social engineering exercise, we would produce a report. So, in this report, we will analyze which departments and how many people have clicked on the links, and we will invite them to attend training.

00:11:03 Interviewer

Okay, got it.

00:11:05 Interviewer

So my second question is, what are your main sources of clients?

00:11:10 TPR6

Uh, our main clients are small and medium-sized enterprises, as well as institution agencies.

00:11:14 Interviewer

Institution agencies like those in the government?

00:11:18 TPR6

Yes, like town offices, county councils, and the Ministry of National Defense.

00:11:22 Interviewer

Okay, let's move on to the third question. What are the main reasons why these clients seek your services?

00:11:32 TPR6

Uh, first, because we are a Taiwanese company, so information security is national security, so most institution agencies choose us because of our MIT background.

00:11:43 TPR6

The other reason is that, for the company, our overall service value for money is good, and local services are better, because if a local vendor needs assistance, they can just call our domestic call center. And also, in terms of equipment resources, we have a higher level of resources. For example, firmware updates do not incur additional costs.

00:12:10 TPR6

Generally, most are subscribers.

00:12:13 Interviewer

Firmware is?

00:12:14 TPR6

Software, it's like application updates, that's firmware updates.

00:12:21 Interviewer

Firmware is the f-i-r-m, right?

00:12:26 TPR6

F-i-r-m, yes.

00:12:28 TPR6

Software updates, you can also say software.

00:12:32 Interviewer

Okay, for the fourth question, I wanted to ask, which aspect of network security do you think most of your clients are lacking in?

00:12:43 TPR6

I think for the majority of the market, or for small and medium-sized enterprises, they already have firewalls in place. Therefore, attack methods nowadays are more likely to come from external to internal. So, we need to focus more on endpoint protection and solutions to address endpoint protection. The endpoint part may include PCs, production equipment, and other devices within the organization. We need to expand our solutions for protection against threats originating from within the organization.

00:13:16 Interviewer

Okay.

00:13:16 Interviewer

Because, as you mentioned earlier, most people now have firewalls.

00:13:24 TPR6

The concept of having firewalls is now widespread.

00:13:26 Interviewer

Yes, but once the firewall is breached, what happens next?

00:13:29 TPR6

Right, because the threat of the firewall comes from external attacks, but the actual threats nowadays are more internal.

00:13:31 Interviewer

What do you mean by internal?

00:13:39 TPR6

When I'm using my PC to browse the internet, if I accidentally click on something, and your PC is on the same network segment as mine, then I could infect your PC. If my PC has a control code, then I could use it as a jumping point to control your computer.

00:13:54 Interviewer

Okay, got it.

00:13:58 Interviewer

Okay, so for the fifth question, I want to ask, what are the main types of network attacks that you have dealt with?

00:14:06 TPR6

Um, let me see the question.

00:14:13 TPR6

Understood. In what situations would customers need to use our solution when encountering network attacks? The first scenario is when their critical servers are possibly under attack, and the second scenario is when their files are encrypted, causing urgency. Another situation is when their email services are disrupted. In such cases, I would recommend utilizing features within our firewall, such as Web Application Firewall (WAF) to protect critical servers, Intrusion Prevention System (IPS) for intrusion detection and defense, and other functionalities like anomaly traffic detection, and so on.

00:14:38 Interviewer

Okay.

00:14:47 Interviewer

Okay, the next few questions are, well, I don't think I designed this question very well, but I still want to ask. So, for the second question, I want to ask, as you mentioned earlier, when network criminals break through the defenses you have set up, and then the next step is to minimize damage and manage the incident, what are the main mechanisms for this?

00:15:20 TPR6

If they have already broken through, then the files may have already been encrypted. Well, if I usually do backups, at least if it is encrypted, I still have a backup and can recover it. Each host should have at least three backups, and the backup method should be done both locally and remotely.

00:15:43 TPR6

Exactly, it's like not putting all your eggs in one basket. In addition to making backups, you may need to take the action of changing your passwords. The reason behind this is that your passwords might be too simple and easily guessed. Also, if you reveal too much personal information publicly, it becomes easier for attackers to exploit your weaknesses. To strengthen your passwords, I would recommend using at least 8 characters with a combination of uppercase letters, lowercase letters, and numbers.

00:16:19 Interviewer

OK, the seventh question is, how would you evaluate the cyber resilience of the technical services provided by your company?

00:16:33 TPR6

What do you mean by cyber resilience? Is it about our unique feature that can maintain these technical services?

00:16:45 Interviewer

Yes, I'm asking because I think my Chinese translation might not be very good. The English term is "cyber resilience," and its concept is somewhat similar to, for example, a building or a company that uses electricity. When you use electricity, you might suddenly experience a power outage, but you have a backup power source that can immediately come in to replenish it so that your company doesn't have to shut down completely. It's like having a backup power supply, but for the internet.

00:17:31 TPR6

So, you mean internet backup?

00:17:32 Interviewer

Yes, or, for example, when you...

00:17:33 TPR6

Because this will be divided into two parts, are you referring to the part when the network is interrupted or when the network is under attack? The ability to restore my host after it has been attacked.

00:17:43 Interviewer

Uh, yes, it's about the restoration ability after my host has been attacked.

00:17:49 TPR6

When the host is attacked, the first thing is that, because actually cybersecurity is layered, from outside to inside and from inside to outside, you have to do it layer by layer. He may have broken through the first layer, but I still have the second layer to protect myself, so at least my losses won't be so great. What we can provide is that we can suggest which part has weaknesses to do a repair, and slowly achieve layer-by-layer protection. Because you certainly can't build everything in place all at once, but for example, if you set up the first firewall today, and you feels that it's not enough, we will suggest to do more. Ah no, it's not that you feels it's not enough, but we see that the content inside has not been segregated, so we will suggest building a second internal firewall. Besides the firewall, there's also the switch, which connects to the wireless network environment. The Access Point (AP) is also part of the network environment. The AP and the switch work together to achieve internal network collaborative defense. It's not just a single action, but rather a combination of measures to enhance security.

00:18:52 Interviewer

Okay, I see.

00:18:59 TPR6

Besides the internal measures already in place, should they also consider implementing identity authentication mechanisms such as two-factor authentication? When personnel connect to the system, they shouldn't be able to log in directly with just a username and password. Instead, they should go through two-factor authentication like Google's or LINE's verification before gaining access. Multi-factor authentication is essential. Additionally, they should consider introducing protective devices for the important organization's frontend.

00:19:30 TPR6

Because if your important host's frontend is vulnerable, attackers may directly encrypt your files and take them away. Have you backed up your data? These are all interconnected and dependent on each other.

00:19:40 Interviewer

Mm-hmm.

00:19:42 TPR6

When the firewall is interrupted, have all these settings files been backed up?

00:19:52 TPR6

How can we recover to the original state as quickly as possible, where all my settings are there, and even if someone copies them and interrupts me, I still have a backup. As long as I have a machine, I can set it up immediately and build the original environment.

00:20:05 Interviewer

Understood.

00:20:07 Interviewer

So, your company will also provide some solutions, such as your current software or you will help design some solutions, which will include this part?

00:20:24 TPR6

Yes, because if we have a plan, we will write a planning document. For example, we will look at the overall network architecture of the area that needs strengthening and provide a suggested solution.

00:20:35 TPR6

This part will include how to do the backup that was just mentioned, how to restore it, and even a plan for disaster recovery drills.

00:20:46 Interviewer

OK.

00:20:48 TPR6

When a disaster occurs, how can I quickly restore it? For example, if there is an issue with the email server, how can I ensure its rapid recovery? The first step is to ensure regular backups. You can use an external USB hard drive as a backup device and perform scheduled backups. In the event of a problem, you can connect the USB drive to another machine, boot from it, and restore the backed-up files, allowing the system to continue functioning without interruption, and ensuring that email services remain operational.

00:21:20 Interviewer

OK, so what I want to ask is, because you just mentioned these, your company provides technical services related to cyber resilience. How would you evaluate your company's offering in this area?

00:21:37 TPR6

I should say that our company is a local information security company in Taiwan. Although we are a Taiwanese vendor, our engineers also have professional certifications. Our company has also passed ISO 27001 certification, so in this area, we actually have professional information security planning and resource capabilities.

00:21:59 Interviewer

OK, great.

00:22:01 Interviewer

We are now on the eighth question. In terms of the technical services provided by your company, which aspect do you think is relatively inadequate? Which part is lacking?

00:22:13 TPR6

Uh, there is a part called log forensics analysis.

00:22:17 Interviewer

Log forensics analysis?

00:22:18 TPR6

Yes, forensics analysis. This is the information in the logs of the firewall. Actually, these logs can be analyzed in more detail, because logs are like records of past history, including the in and out logs that may be generated every day, and these logs may only be understood by R&D. But because our domestic company has limited manpower, it is difficult to do this analysis every day. Only foreign vendors may have the manpower to do support. I think this is the lacking part, and there is another part.

00:23:00 Interviewer

Log forensic analysis?

00:23:03 TPR6

And then there is an endpoint solution, because a company may have 200 computers, and each computer may have such a detection software installed. When it triggers a threat, it can immediately report back to the server side for real-time response. This thing requires more manpower to maintain, so I think these two areas are lacking.

00:23:32 Interviewer

Okay, so we come to the 9th question. What do you think can be done to improve these deficiencies in terms of the two points you just mentioned?

00:23:44 TPR6

The deficiency in this area is that the expertise of every cybersecurity company is different, because cybersecurity is layered and not just a single layer. So every company's expertise is different, and we can cooperate with partners to find solutions together.

00:24:01 TPR6

For example, I mentioned earlier that if I don't have a solution like EDR or NDR for endpoint protection, I can collaborate with a partner and integrate their software with my firewall for joint defense. We can discuss such cooperation.

00:24:20 Interviewer

Okay, so I want to ask, is your company more like providing front-end services?

00:24:25 TPR6

We focus mainly on the gateway side.

00:24:28 Interviewer

So you are lacking in the EDR and NDR areas that you just mentioned?

00:24:33 TPR6

Yes, EDR and NDR are endpoint engines, yes, for identification.

00:24:35 Interviewer

OK.

00:24:40 Interviewer

You said you focus on gateway?

00:24:42 TPR6

Yes gateway, and a gateway is the first checkpoint when you come in and out. So we actually do firewall gateways or email gateways.

00:24:55 Interviewer

OK, understood.

00:24:57 Interviewer

So you think it might be possible to collaborate with other companies?

00:25:01 TPR6

For example, let's say within the firewall, there is antivirus software, and we also collaborate with Kaspersky to complement its capabilities. Similarly, if I need application control, I can collaborate with third-party application databases to enhance the control measures.

00:25:22 Interviewer

OK, good, anything else you want to say?

00:25:25 Interviewer

I mean except for improving the shortcomings.

00:25:33 TPR6

There are mainly these two.

00:25:34 Interviewer

Okay, then let's move on to the tenth question. Do you know if your company has any plans to improve or expand the technology services you provide in the future?

00:25:52 TPR6

Expanding our services would involve focusing on customized cybersecurity solutions because many threats and requirements are personalized and specific to individual enterprises. We aim to provide services tailored to each company's unique needs. Uniform standard solutions are already widely available in the market, which is relatively narrow. In the field of cybersecurity, hackers target specific enterprises, and they won't use the same approach for every company.

00:26:29 Interviewer

Okay, I see.

## Section G

00:26:29 Interviewer

Moving on to section G, we will discuss the issue of collaboration between the public and private sectors. The first question is... In your opinion, would collaboration between the public and private sectors, such as your company, be beneficial for the development of cybersecurity?

00:26:52 TPR6

Currently, many regulations are issued by the government and followed by the private sector.

00:27:00 TPR6

Therefore, collaboration between the public and private sectors is already happening in the field of cybersecurity.

00:27:08 Interviewer

So, you think in this way, it is?

00:27:11 TPR6

think it is necessary because cybersecurity is national security, as mentioned earlier. Therefore, the government should take the lead in guiding some aspects of the private sector.

00:27:18 Interviewer

Moving on to the second question, based on your knowledge, what are some mechanisms or models of public-private sector collaboration in the overall cybersecurity field in Taiwan?

00:27:35 TPR6

Actually, as mentioned earlier, the government will enact laws, such as the Cyber Security Management Act, which requires ABCDE-level agencies to carry out certain tasks. However, who will carry out these tasks when agencies become aware of them? It will be the private sector companies that will be contracted to perform these tasks. For instance, under the Cyber Security Management Act, vulnerability scans, including host and web, are mandatory for agencies rated C or above. Additionally, social engineering exercises are required, and the firewall must contain specific functions, such as IPS intrusion detection and WAF, which stands for web application firewall.

00:28:26 TPR6

So these things are all basic requirements.

00:28:29 TPR6

So, as I mentioned earlier, the public and private sectors have always worked together in this regard.

00:28:38 Interviewer

OK.

00:28:39 Interviewer

So, moving on to the third question, following up on the second one, how do you evaluate the current model and mechanism of collaboration?

00:28:50 TPR6

Actually, I feel that our revenue is driven by government regulations and compliance requirements.

00:28:55 TPR6

Exactly, because when the government takes the lead in implementing these measures, the budget becomes available. With allocated budgets, not only government agencies but also businesses will understand the legal requirements and importance of implementing these security measures regularly.

00:29:12 TPR6

That's right. Even in the case of enterprises, the industry leaders like TSMC, for example, have their own internal regulations and standards to comply with. In the semiconductor industry, the regulations related to information security are very similar to the Cyber Security Management Ac. They cover aspects such as email filtering requirements and the necessity of implementing authentication mechanisms like DKIM, SPF, and DMARC.

00:29:33 TPR6

Firewalls are the same too. Without these regulations, things would not be so coordinated. This thing is bound together by public and private sectors, and government and private things are tied together.

00:29:47 Interviewer

So, do you think that the current level of cooperation is still acceptable?

00:30:00 TPR6

Yes, especially in recent years, it has had a lot to do with political factors. Because now, can I talk about it? It doesn’t matter, right?

00:30:07 TPR6

Yes, that's correct. Currently, the ruling party is the Democratic Progressive Party (DPP), and they are more inclined to support Taiwan's domestic products and industries. For government agencies, promoting domestic brands and companies would be advantageous as it strengthens the local industry and provides more opportunities for them. It makes a significant difference in the government's promotion of national products compared to other alternatives.

00:30:22 Interviewer

Okay.

00:30:24 Interviewer

So, have you encountered any difficulties in the cooperation you know about?

00:30:32 TPR6

What kind of difficulties? Well, the difficulties lie in the fact that the information landscape is highly open-ended. For example, the Ministry of Digital Affairs, which handles digital information, introduced a zero-trust solution. However, understanding and following such a solution can be challenging as it requires comprehensive knowledge about what it entails. Moreover, in the case of EDR and NDR, which the Ministry of Digital Affairs also promotes, implementing and maintaining these solutions can be costly and resource-intensive.

00:31:05 TPR6

General enterprises may not be able to afford it, so it may be difficult for private and small and medium-sized enterprises to implement it. It may only be easier for large organizations to accept such solutions.

00:31:21 Interviewer

So, it's a bit like the government is too idealistic, but in practice, there are some actual difficulties for the organizations to implement it.

00:31:31 TPR6

In terms of difficulties, yes. Or, for example, when they develop a new cybersecurity protection solution today, whether it can be compatible with existing operating systems. Like a few years ago when the government introduced GCB and VANS.

00:31:44 TPR6

GCB and VANS are similar to asset inventory systems, but they are software. However, when installed on PCs, there were often compatibility issues or crashes, causing operational difficulties.

00:31:59 Interviewer

So, since there are these difficulties, how do you think we can improve these difficulties in the future?

00:32:08 TPR6

How can we improve these difficulties?

00:32:10 Interviewer

What direction can we go towards? Your own ideas?

00:32:16 TPR6

The first point is that with software, it often starts with some bugs or optimization needs, but over time, it improves. So, everyone needs to upgrade the old firmware as well. In fact, everything should be integrated from the inside out. When we develop new software, we need to optimize it, and at the same time, update the old software, so that they can work together seamlessly.

00:32:42 Interviewer

OK, so as you mentioned earlier, the government may have more idealistic plans, while businesses may face practical challenges in implementation. It's like there's a gap between the ideals and the reality.

00:32:53 TPR6

Yes, exactly. For example, the government may advocate certain initiatives and set ambitious goals, but private enterprises might feel that those initiatives are distant from their current situation or operations. This can create a disconnect between the government's vision and the practicality for private businesses.

00:33:01 Interviewer

I understand. So how do you think we can improve or solve this generation gap issue?

00:33:15 TPR6

Because this is actually a bit macroscopic, as you mentioned earlier, if a company is publicly listed or traded, and if something is attacked or encrypted, they will definitely consider all possible solutions and try them out. However, if it's a small enterprise, they might not care much if their data is encrypted. They might just let it go because they don't think their encrypted files are valuable enough.

00:33:38 TPR6

They might prefer to rebuild it. So, I think this part really depends on the type of business and its priorities.

00:33:45 TPR6

Because this gap actually exists in how you perceive the value of this data. Whether you consider this data important or not is related to its value.

00:33:59 TPR6

Because whether it's the government or an enterprise, the most important thing is operations, so the most important things are money or their confidential know-how, right?

00:34:11 Interviewer

So it also depends on the enterprise. The government may be emphasizing this point, but some businesses may not care about it.

00:34:18 TPR6

They may think their data is not valuable, so they don't care if they are attacked.

00:34:25 TPR6

But if they think their data is important, it may be affected by some news events, and they will think about planning for this, especially for enterprises with IT departments.

00:34:37 Interviewer:

So it seems like it also needs to be customized?

00:34:43 TPR6

How can we narrow this gap? One way to do it is by increasing internet accessibility and promoting more digitization of services. As internet usage becomes more widespread and everything becomes more connected, the gap may gradually close. However, it's also influenced by regional factors. For example, there might be differences between Taipei and Nantou, where Taipei is more likely to have a stronger awareness of cybersecurity.

00:35:06 Interviewer:

What do you think the government or enterprises can do since there is such a gap?

00:35:10 TPR6

First, increase promotion and advertisements, such as making videos. For example, internet ATMs or online banking is prone to cybersecurity vulnerabilities, but as more people use online banking, they will become more aware of cybersecurity. When cybersecurity is relevant to people's daily lives, they will pay more attention to it. In the past, people thought it had nothing to do with them, but now everyone has a smartphone, so cybersecurity is becoming increasingly important.

00:35:43 Interviewer:

So the government also needs to promote and advertise more?

00:35:46 TPR6

Yes, the more you are exposed to it, the more you see, the more you have a concept of it, and the more you want to change something.

00:35:55 Interviewer:

So it's natural?

00:35:56 TPR6

Yes, the awareness will increase, but it has to keep appearing frequently.

00:36:02 Interviewer

So let's move on to the fourth question. Actually, the fourth question is about what you think can be improved, but I already asked about that earlier.

00:36:11 TPR6

Yes, I’ve answered that.

00:36:13 Interviewer

You did answer, but did you prepare for this question in advance?

00:36:18 TPR6

I prepared? What do you mean?

00:36:20 Interviewer

Yes, didn't you take notes earlier?

00:36:23 TPR6

Actually, I think that’s everything I want to share.

00:36:25 Interviewer

OK, I just wanted to make sure that you had the opportunity to say everything you wanted to say.

00:36:30 TPR6

No, I think I covered everything.

00:36:32 Interviewer

Okay, then let's move on to the fifth question. Earlier we talked about Taiwan as a whole, but now that you're working in this unit, which focuses on internet security, do you have any experience of cooperation between public and private sectors in this area?

00:36:47 TPR6

Let me think. Cooperation?

00:36:51 Interviewer

Yes, any kind of cooperation in internet security between private enterprises like yours and public organizations.

00:37:03 TPR6

Do you mean cooperation in terms of developing projects together?

00:37:06 Interviewer

Yes, that's right. Any kinds of collaboration.

00:37:09 TPR6

Uh, for example, we have assisted the Industrial Bureau of the Ministry of Economic Affairs in establishing an OT field validation mechanism.

00:37:20 TPR6

So, we collaborated with them to conduct a test. They set up a cybersecurity verification environment, and we provided the necessary equipment for this verification mechanism to see if it could pass their validation process.

00:37:37 Interviewer

Okay, then let's move on to the sixth question. What is your evaluation of the current collaborative mechanism with them?

00:37:48 TPR6

As for how to evaluate it, actually, it allows us to simulate a real attack and do a simulation of a protection mechanism.

00:37:59 TPR6

Yes, so we know what kind of attack techniques they might use, and we play the roles of the attacker and defender to test this verification mechanism.

00:38:14 Interviewer

Then you can, it's like targeting the network, and you might understand it better, right?

00:38:21 TPR6

Yes, we will know what kind of threats there might be in your current domain and what kind of situations you might encounter.

00:38:29 TPR6

In some scenarios, the threats might occur in production lines, while in other situations, they could target critical infrastructure or various types of businesses. Additionally, there could be incidents of threats in data centers or server rooms within government agencies.

00:38:43 Interviewer

So do you think the current mode of cooperation between you and them is good? Or do you think there is room for improvement?

00:38:50 TPR6

Actually, their mode of cooperation is probably to promote cybersecurity.

00:38:54 Interviewer

Um, who is trying to promote cybersecurity?

00:38:58 TPR6

Um, the government department. The cooperation I just mentioned is actually the government department trying to promote cybersecurity and finding private entities to collaborate with and demonstrate this.

00:39:10 Interviewer

Do you think this kind of collaboration model is good or not?

00:39:13 TPR6

This collaboration model?

00:39:13 Interviewer

Yes, what do you think?

00:39:16 TPR6

I think it would be better to let more people know because sometimes...

00:39:19 Interviewer

You mean it needs more promotion?

00:39:21 TPR6

Yes, more promotion, because most of the participants are government officials, and the public may not be aware of these messages.

00:39:28 Interviewer

So your collaboration is to help them do what you just mentioned for the Ministry of Economic Affairs.

00:39:35 TPR6

Yes, for the Industrial Development Bureau.

00:39:36 Interviewer

Okay, then they will hold something like a seminar or something like that, right?

00:39:42 TPR6

No, they provide a smart manufacturing venue. And there will be some equipment related to smart manufacturing, such as PLCs, indicator lights, and so on.

00:39:53

Mm, hmm.

00:39:54 TPR6

They will simulate scenarios in which the system gets attacked by hackers and then evaluate the defense mechanisms that can be implemented. As a defense solution provider, we offer gateway solutions, and we will provide a device for testing whether the different aspects pass the verification process.

00:40:09 Interviewer

OK, then they will provide this information to some...?

00:40:13 TPR6

They provide this information to some enterprises that need a solution.

00:40:18 Interviewer

OK, but only to enterprises, not to the public?

00:40:24 TPR6

Yes, not to the public, because the public doesn't really understand this.

00:40:31 Interviewer

But do you think the public also needs to understand this area?

00:40:36 TPR6

For the public, it's more about how to promote it to make the public interested. Even if you let the public know about this, they will still feel that it has nothing to do with them.

00:40:47 TPR6

Perhaps the bosses will be more interested and can invite the bosses of various enterprises to come and visit.

00:40:56 Interviewer

So, have you encountered any difficulties in your cooperation so far?

00:41:02 TPR6

Encountering difficulties in cooperation is because everyone's ideas may differ. For example, the resources provided in the specified field that we need to connect to may have some differences, so continuous meetings and discussions are required to address the integration issues.

00:41:19 Interviewer

So, it's kind of like, it's related to people?

00:41:23 TPR6

Yes, it's related to people. We need to have meetings to discuss it, because, for example, the people in the laboratory and those in the industry may have different ideas. They may have idealistic thoughts, but we may have difficulties executing them.

00:41:42 Interviewer

So, in that case, where do you think we can improve this problem?

00:41:46 TPR6

It depends on which side is the main controller. We need to see which side can lead everything and have the most influence.

00:41:55 Interviewer

Um, do you mean someone should take the lead on one side and have frequent meetings like this? To facilitate more communication?

00:42:04 TPR6

Yes, for example, if you really want to achieve certain results in the executable part, and you want to know how to achieve these results, then one side should take the lead and set the direction.

00:42:19 Interviewer

Is that side the government?

00:42:21 TPR6

Um, not necessarily. It could be the government if their method is more feasible. We should discuss and see which side's method is better to implement.

00:42:32 Interviewer

OK.

00:42:34 Interviewer

So, what you're saying is that currently, the difficulties encountered in cooperation are all due to people having different concepts, as mentioned earlier?

00:42:41 TPR6

Yes, that's right. Actually, the internet is ultimately created by people, so everything is related to people.

00:42:49 Interviewer

So, if we want to improve the situation, you hope that someone can take the lead and communicate more?

00:42:58 TPR6

Yes, because when it comes to collaboration, there are always new things involved, and there will inevitably be some problems.

00:43:08 Interviewer

OK, so is it like the government is a bit like the people in the laboratory, and you are more like the industry?

00:43:12 TPR6

That's correct. He may suggest, "Why don't you simulate various environments and showcase it that way? It will have a significant impact." However, in reality, it's challenging to execute and demonstrate effectively.

00:43:23 Interviewer

OK, got it.

00:43:24 Interviewer

So, the solution is to communicate more with them?

00:43:29 TPR6

Yes, that's right. Communication is the only way to solve it.

00:43:34 Interviewer

What do you think could be improved in terms of cooperation?

00:43:40 TPR6

It's the cooperation part.

00:43:43 TPR6

Government cooperation is usually project-based.

00:43:45 Interviewer

Projects.

00:43:46 TPR6

For example, they have something they want to promote.

00:43:52 TPR6

For example, there is a platform similar to a cloud marketplace where we can offer our own cybersecurity solutions. Private companies can place their cybersecurity solutions on this cloud marketplace for sale. The marketplace might operate on a points-based system, where enterprises purchase points and then use them to buy solutions from the government platform.

00:44:13 TPR6

But we are also discussing how to do this.

00:44:18 Interviewer

Okay.

00:44:19 Interviewer

Let me check.

00:44:24 Interviewer

Okay, I think that's about it for today.

00:44:31 Interviewer

Thank you.