# Transcript

## Section A

00:00:00 Interviewer

So now we will begin the interview with TPU5. Let's start with section A. The first question is, as you work in the public sector, there is no doubt. The second question is, where are you currently working?

00:00:17 TPU5

I work in the [a government criminal investigation unit]. I have been working here for about two and a half years.

00:00:27 Interviewer

Two and a half years.

00:00:29 TPU5

My job title is police officer. Currently, I am responsible for handling information security incidents, as well as researching and developing in virtual currencies and emerging technologies.

## Section B

00:00:43 Interviewer

Wow, virtual currencies. OK, got it. So now we move on to section B. These three questions are related to Taiwan's overall cybersecurity issues. The first question is, based on your understanding, what are the main types of cyberattacks that Taiwan is currently facing? And what are the methods used? Can you give some examples?

00:01:09 TPU5

So currently, it's multifaceted, right?

00:01:14 TPU5

So should I focus on just one main attack?

00:01:18 Interviewer

No, you can talk about all of them.

00:01:21 TPU5

Because currently, criminal groups, such as fraud rings, mainly focus on obtaining money through crimes. So they need to obtain personal information first to be able to commit crimes. Therefore, these criminal groups may have some connections with hackers. Hackers may attempt to obtain personal information by targeting the web or database components.

00:01:54 Interviewer

I see.

00:01:56 TPU5

So most of their attacks are SQL injection, which exploits various vulnerabilities on websites to execute commands.

00:02:13 TPU5

As for examples, um...Can talk about it?

00:02:21 Interviewer

You can decide for yourself. If you feel uncomfortable discussing it, you don't have to.

00:02:23 TPU5

Because some companies such as small and medium-sized enterprises, they do not have comprehensive cybersecurity protection measures, and their budgets for this are not high. They can only do basic related things like router or firewall settings. They do not have protection against attacks on the application layer of the OSI seven-layer model. Therefore, in the case of SQL injection, if their computers have vulnerabilities, they are almost inevitably directly attacked, and their data is likely to be stolen.

00:03:00 Interviewer

Hmm.

00:03:04 TPU5

Okay, then there is social engineering. Hmm, social engineering involves using emails or SMS, as mobile phones are now very developed, to send phishing links that trick you into entering your personal information. It can also involve sending malicious programs to your mailbox to obtain your personal information or to implant malware. In the case of malware, the attacker can control your computer remotely, and in severe cases, they may use RCE (Remote Code Execution) to gain access to your computer.

00:03:53 Interviewer

Hmm, you mean that's called RCP?

00:03:55 TPU5

Uh, maybe RCE is more accurate, because it stands for remote.

00:03:56 Interviewer

Okay, okay.

00:03:58 Interviewer

So it's like remote control, right? OK, OK.

00:04:02 TPU5

Yes, remote control, and they can intercept some of your computer data and screen.

00:04:10 TPU5

Those are probably the two more severe cases.

00:04:13 Interviewer

Hmm.

00:04:14 TPU5

The others are not that serious, in my opinion.

00:04:17 Interviewer

OK. For the second question, what do you think are the main targets of cyber attacks in Taiwan right now? And what are the reasons behind them? Why have they become targets of attack?

00:04:31 TPU5

Um, there are two aspects to this. Firstly, as I mentioned earlier, criminal groups need personal information to carry out their fraudulent activities, which is the same as the previous question. Secondly, I think it's a political factor, an international political factor. Regardless of what's happening in China, for example, there have been a lot of incidents here since the Pelosi incident last year in August 2022, whether it's IoT attacks or website tampering. I think these are the two main reasons.

00:05:12 Interviewer

Mhmm, I see.

00:05:16 Interviewer

These two factors ? So these two factors, um, because what you just said were more likely related to the third question, which is about your perception of factors that impact cyber security in Taiwan...

00:05:26 TPU5

Right, what do you mean by targets?

00:05:29 Interviewer

For example, like the MRT…

00:05:34 TPU5

Public institutions?

00:05:35 Interviewer

Yes, or which industry?

00:05:37 TPU5

The targets are not limited to any specific industry. Any e-commerce website is a target because it contains transaction information. They use social engineering techniques like calling or texting you directly and then use the transaction process to, for example, use installment transfers and so on.

00:06:06 Interviewer

I see, got it.

00:06:08 TPU5

Then I think it's mainly shopping websites. The second one is, if it is due to political reasons, it may be government departments. They may invade government departments and replace relevant information. For example, last year, the entire website of the Office of Academic Affairs at National Taiwan University was replaced with the flag of China.

00:06:33 Interviewer

Mhmm, I see.

00:06:35 Interviewer

National Taiwan University's Office of Academic Affairs? OK.

00:06:39 TPU5

We and the Investigation Bureau have investigated this.

00:06:41 Interviewer

Mhmm, I see.

00:06:43 Interviewer

Was that after the Pelosi incident?

00:06:46 TPU5

Yes, after. It was on August 2nd, or around the end of August, yes. This was reported in the news, so I am not afraid to talk about it.

00:06:57 Interviewer

Haha, no problems.

00:06:59 TPU5

Uh, right. Then, does what I just said become the answer of the third question?

00:07:03 Interviewer

Yes, and you can talk more if you think there's more.

00:07:08 TPU5

There's not much to say, but I think apart from these two factors, there are already very few hackers who do this just to show off their personal skills.

00:07:26 Interviewer

Already very few this kind of hackers?

00:07:27 TPU5

They (the hackers) are always like this. For example, with regards to network security and DDOS attacks, you need to actively attack. Actually, we don't know the reason behind it. Like yesterday's MRT, ah, no it wasn't MRT. It was YouBike. I suspect it was a DDOS attack because the connection was interrupted and then it worked again after restarting. That's very likely a DDOS attack, but it wasn’t reported. They just said it was a system issue.

00:08:01 Interviewer:

Hmm.

00:08:07 TPU5

I think apart from these two factors, there aren't many other factors. It's either fraud or a fraud syndicate, or it could be political factors.

00:08:15 Interviewer:

Hmm, okay.

## Section C

00:08:16 Interviewer

I understand. Now we're on section C. The first question in section C is about the issue of integrity. Based on your understanding, what plans does the Taiwanese government currently have in place for internet security? And do you think these plans are good or not?

00:08:34 TPU5

The first thing is that…The overall plan is that our top-level part is cybersecurity, which is the Cyber Security Management Act.

00:08:42 TPU5

This is the top-level plan, but it is currently being managed by the Ministry of Digital Affairs.

00:08:46 Interviewer

Okay.

00:08:47 TPU5

It may be integrated, um, previously it was managed by the Ministry of Economic Affairs, but now all the departments are managed within the Ministry of Digital Affairs. Um, regarding this, I actually took a look at their plan, which is mainly focused on blue team, which is the protection plan for the defense team.

00:09:12 Interviewer

The blue team is for defense, and the red team is for attacks?

00:09:14 TPU5

Yes. The defense plan for the blue team is actually not enough just to let the IT personnel know how to defend themselves. And then how to manage the security incident? Um, actually it is very vague, and the notification process for security incidents is also very vague. You have to report it within an hour, but um, in many operational aspects, the Ministry of Digital Affairs does not know when your agency was invaded. Even if you report it a month later, they still do not know. Although there will be a log mechanism, um, in fact, it is difficult to go to various agencies or departments to see if there have been any invasions. There is a lack of manpower and professional level.

00:10:14 Interviewer

Mm-hmm.

00:10:16 TPU5

Then, wow, um, the overall plan didn't include these because I see the plan is to report within one hour, then dispose of it within 36 hours, within 72 hours. Then, after the disposal, then what?

00:10:33 Interviewer:

Hmm.

00:10:36 TPU5

Regarding the investigation or responsibility of a cyber security incident, it is said that the responsibility lies with the Ministry of Digital Affairs. However, if it involves the public sector, because we are a law enforcement unit and an investigative unit, we must immediately investigate if there is any criminal activity, as stipulated in Article 228 of the Criminal Code.

00:11:01 Interviewer:

Hmm.

00:11:02 TPU5

So when we know it involves a public sector entity, such as the Office of Academic Affairs at National Taiwan University being attacked, we need to do something about it. And they need to report it separately to the competent authority of the Ministry of Education, and then the Ministry of Education will report it to the Ministry of Economic Affairs.

00:11:12 Interviewer:

OK.

00:11:23 TPU5

This means that it will become two separate lines of investigation, one for us and one for them, without an overall plan and without centralized resources. And these resources and manpower are also scattered. Hmm, this is my personal evaluation, so I have always felt that the lack of talent is also a reason. However, your professional level is only in the defensive part, then how do you know how to attack?

00:11:48 Interviewer:

Hmm.

00:11:57 TPU5

Most of our IT personnel don't know how the attack came in. This is what I have encountered in terms of cyber security incidents.

00:12:09 Interviewer

Ok, then let's move on to the second question. Questions two and three can be answered together, which is about the current strategies for preventing internet threats.

00:12:27 TPU5

Is it the government's perspective or my own opinion on what should be done?

00:12:31 Interviewer

It's about the government's current strategies.

00:12:34 TPU5

Currently, the government's strategy is that the Ministry of Digital Affairs has a platform for information sharing. It's a platform for reporting any threats you encounter on the internet, and then you can notify everyone.

00:12:45 Interviewer

I see.

00:12:48 TPU5

But when all the IT personnel in the public sector see it, they are like….but what does it mean? You know what I mean? They will be like, ok….. we need to update certain equipment, but we have no idea how the attack was carried out. So, can the protection measures we implement prevent us from being attacked? In fact, we cannot prove it. Therefore, I believe that we need to continuously improve our technical level in order to improve in this aspect.

00:13:25 Interviewer

I see.

00:13:26 TPU5

For example, with Windows, the technical level of information security personnel. And in other countries, everyone is doing CTF (Capture the Flag).

00:13:41 Interviewer

I see.

00:13:48 Interviewer

But currently, we don't have that in Taiwan yet?

00:13:50 TPU5

We have it, but it is limited to universities. You are not promoting things like red teaming or penetration testing. Penetration testing and red teaming are actually quite similar, but our information security personnel don't really understand them, or I should say, our information technology personnel don't really understand them.

00:14:16 TPU5

Because in the public sector, information security personnel are information technology professionals who undergo further training, I think the level is far from enough, no matter which department it is. Like me, I am constantly learning, hmm.

00:14:26 Interviewer

Hmm.

00:14:31 TPU5

It's just that his scope is too broad. The scope of information security is really too broad, and if you want to focus on a certain area, you have to put in a lot of effort.

00:14:44 Interviewer

OK, so you think that the area that needs to be improved is still on people?

00:14:50 TPU5

I think it should be based on its industry value or, like, if it is a shopping website that has been hacked, then most of it is web-based, so you should focus on the security of the web.

00:15:13 Interviewer

Mm-hmm.

00:15:14 TPU5

It could be IoT, like last year when the advertising screens in 7-11 were replaced.

00:15:25 Interviewer

During the Pelosi ransomware attack?

00:15:29 TPU5

Do you know why? Oh, a very simple reason. He just read a test file from a certain website and uploaded that test file to replace it.

00:15:46 Interviewer

So it was easy to replace?

00:15:48 TPU5

Yes, it's that simple.

00:15:51 Interviewer

So it means that maybe 7-11's defense in this area is also insufficient, and it is easy to...

00:15:56 TPU5

Yes, completely insufficient.

00:15:59 TPU5

Hmm, they were too careless, thinking that, hey, how could he possibly know how to replace it?

00:16:03 Interviewer

I understand. Because actually, my understanding of this information is mainly from literature. I don't have the same level of understanding of cybersecurity technology as you do. What I understand is mainly about some industries. They may directly hire IT personnel to do cybersecurity work. But, IT personnel and traditional cybersecurity personnel may have different knowledge. But many companies may not have attached importance to this area and simply hire IT personnel to do cybersecurity work, which may result in their lack of understanding and proficiency in this area when they have to do it.

00:16:45 TPU5

Well, what you said about the difference between IT and cybersecurity personnel is not really a difference. IT personnel build their knowledge on basic information, and cybersecurity personnel build on top of that to further engage in cybersecurity. So cybersecurity personnel must have a foundation in information. If you suddenly switch to cybersecurity without any knowledge in network, Linux, programming languages, etc., it's not possible.

00:17:19 Interviewer

I see.

00:17:23 TPU5

Yes, so you must have a foundation in information, in my opinion.

00:17:25 Interviewer

You must have a foundation in information and then enhance your knowledge in cybersecurity?

00:17:29 TPU5

Yes, enhance your knowledge in cybersecurity. However, because there are few cybersecurity companies in Taiwan. Many industries need cybersecurity personnel, and they expect them to know everything. But that's not possible.

00:17:51 Interviewer

Right, it's not possible.

00:17:55 TPU5

Yes, it's not possible. It's not that simple. When a company is under attack, they expect you to know everything.

00:17:59 Interviewer

I see.

00:18:01 TPU5

Of course, from the company's perspective, it's natural for them to do that. But they are too naive.

00:18:10 Interviewer

So let's move on to the fourth and fifth questions. Because we talked about prevention earlier, now the fourth question is about what the current strategies are for governments and public agencies when facing network attacks. What do you think of these strategies? And where can improvements be made?

00:18:30 TPU5

Is it about practical aspects or regulatory aspects?

00:18:32 Interviewer

Both can be discussed. I think it's similar to what you just mentioned, many cybersecurity personnel may not understand the source of the attacks at all. So when the attack happens, they may not know what to do. Can you explain this?

00:18:48 TPU5

The first thing is that, for network attacks, such as service interruptions, network interruptions, system interruptions, or there may be different strategies. For network interruptions, you may need to check the traffic or whether the service provider of the ISP network is interrupted or if the traffic is too high and is clogging certain applications. Or is it really an attack? This is the network part.

00:18:53 Interviewer

Hmm, I see.

00:19:18 TPU5

For the system part, it's the same. Has it been clogged by too many requests? Is it down? Probably like that. As for the many cases of personal information leakage, they were invaded, and the whole thing was taken away by SQL injection, but they didn't know.

00:19:39 Interviewer

Right, they didn't know?

00:19:40 TPU5

They had no idea at all. It's always the victim who calls and says, "Hey, do you have any installment payment cancellation service?" or "Do you have any kind of service like that?" Then they realize that the personal information has been leaked.

00:20:02 Interviewer

Right, many online shopping platforms are like this now.

00:20:03 TPU5

That's right, so they don't really know how to defend themselves. The basic defense is of course to go to the equipment on the 7th layer of the network, you need to purchase equipment up to the 7th layer.

00:20:17 Interviewer

What is the 7th layer?

00:20:19 TPU5

It's the OSI seven-layer model, the application layer. For the application layer, you need to add equipment, yes, network detection, intrusion detection systems, and intrusion prevention systems are all necessary.

00:20:32 Interviewer

OK.

00:20:34 TPU5

It's different, intrusion detection can detect if there are malicious programs trying to steal your information through your commands. Whereas WAF (Web Application Firewall), an application layer firewall, it to examine whether it is implemented differently, and whether the application layer programs can cause any harm.

00:20:55 Interviewer

So what you just mentioned, um, did you mean that the ability of detecting the malicious programs is still acceptable but maybe improvements are needed in the application layer?

00:21:14 TPU5

Are you talking about most of them? When you face it? Actually, for the public sector, most of them have it, and the public sector uses their own network, which is separate from the general network, yes, so usually they won't encounter it, the public sector usually won't encounter it.

00:21:35 Interviewer

You mean they won't encounter attacks?

00:21:38 TPU5

Um, they won't encounter attacks like DDOS, because they've already blocked it at the front-end with Chunghwa Telecom. If you're talking about substitution, that's application layer. It's HTTP, which is at the application layer. For the application layer, you can specify the front-end and make modifications. If there are vulnerabilities, you can make modifications. Some, like PHP's sequel injection, if you have it….hmmm…. if you don't do the what… hmmm… command retrieval for protection, you may be attacked with sequel injection commands or file uploads. If you upload a shell, it's a, it's a command prompt.

00:22:41 TPU5

Do you know about shell?

00:22:45 Interviewer:

No, I don't.

00:22:47 TPU5

When you upload it, it can directly remote control your computer. With a command or a Trojan horse, the vulnerability of the program is that you eval() its program one by one. For PHP, if you download it, modify it, and upload it to the website, you will open the portal and be able to remotely control the program with commands.

00:23:19 Interviewer:

So this shell is like...?

00:23:21 TPU5

Shell and a Trojan horse.

00:23:24 TPU5

You can google more about it later.

00:23:25 Interviewer:

I may not be very familiar with this kind of technology. I only learned about it from some social sources, so that's why I want to interview you.

00:23:36 Interviewer

OK, let me check. We were on the fourth or fifth question. About what you mentioned earlier, where do you think improvements can be made? So, let’s move on to the fifth question. You talked mostly about response strategies, and these strategies might be easily…., like what you mentioned earlier about being attacked by a Trojan horse easily. How can we improve on that?

00:24:06 TPU5

I think the government department's supervisor needs to understand that not all invasions are harmful. It's only critical systems that can cause harm. If a critical system is compromised, then your personal information might leak out, or the service might not work, or it might be modified. Some modifications, like what happened at the Office of Academic Affairs at National Taiwan University, don't matter much. As long as you can restore it, then it's all good. Has it been compromised? Yes, it was modified but is it important? It's only important for reputation.

00:24:56 Interviewer

Oh, right, reputation.

00:24:57 TPU5

Reputation is important, but from a cybersecurity perspective, it's not important at all because nothing has been stolen.

00:24:57 Interviewer

Hmm.

00:25:07 Interviewer

So there is no actual loss?

00:25:08 TPU5

No actual loss, and as for replacing it, well, it's impossible to have all websites be static. If you use a static website, then you won't be hacked or modified, but that's impossible.

00:25:27 TPU5

I think these supervisors need to increase their knowledge of cybersecurity, not just pay lip service. That's what I think.

00:25:37 Interviewer

Right, but it's the higher-ups who are less knowledgeable.

00:25:40 TPU5

They don't understand at all, and they just say, "Oh, it is a big deal that you were invaded." But for the example of National Taiwan University, I don’t think it's important. Although it is important to maintain a good reputation, I don't think it matters much. In terms of the attack aspect, it didn't really lose anything. It's just a static website.

00:26:03 Interviewer

So for cases that result in actual losses, how can improvements be made?

00:26:09 TPU5

A shopping website, for example, a shopping website or one that involves transactions, it's not a government agency. It's a foundation or an association, like a sports association.

00:26:36 Interviewer

Oh, like the Taiwan Road Running Association?

00:26:38 TPU5

Hey, how did you know that our deputy mentioned it earlier?

00:26:43 TPU5

Other foundations have also been hacked, and in terms of their infrastructure, first, their basic infrastructure is poor, second, they do not have an information security management system, and third, they do not have information security personnel. I think these three points are completely insufficient.

00:27:08 Interviewer

So these three points need to be strengthened?

00:27:10 TPU5

Start with the basics, and then you can talk about how to become more advanced. I think these three are the most fundamental.

00:27:17 Interviewer

Okay, let's move on to questions six and seven. Earlier, we talked about attacks while they were happening. Question six is about what measures government and public agencies take for reflection and review after the attack. Do you think their current measures are sufficient for preventing future attacks?

00:27:43 TPU5

I'm not sure what they did after being attacked because our law enforcement unit's goal is to catch the suspect and to do the investigation, not what they do after the attack. Of course, many companies ask us for advice on what to do, and we offer some suggestions.

00:28:16 TPU5

Besides insufficient infrastructure, implementing an information security management system might mean restricting USBs or preventing users from clicking on emails from unknown sources, which relates to social engineering.

00:28:47 Interviewer

Social engineering.

00:28:50 TPU5

if someone wants so target you with a DDOS attack, there is no way to defend against it. However, you can take preventive measures, such as applying for a CDN (Content Delivery Network) to clean the traffic. This can be purchased in advance from internet service providers. But for small and medium-sized enterprises, their budgets are completely insufficient, and it is impossible for them to do so. Therefore, I think it is more practical to plan according to your industry and budget resources.

00:29:29 Interviewer

Okay, got it.

00:29:32 Interviewer

Okay, so what you just said might have answered the seventh question. So, it’s better to plan individually for different industries? Okay, let's move on to the eighth question. What do you think about the general public's awareness of internet security? Is it sufficient?

00:29:52 TPU5

It's just slogans. They're all just slogans. They don't really understand it.

00:29:59 Interviewer

Hmm, you mean the general public?

00:30:01 TPU5

Ah, for the general public, they would feel that if they were invaded, it's because the government didn't do a good job. But they don't know how they were invaded or why they received government support. They think that they pay a lot of taxes, and the government should do better.

00:30:15 Interviewer

I see.

00:30:16 TPU5

This is a completely wrong idea, in my opinion.

00:30:19 Interviewer

Okay.

00:30:20 Interviewer

For themselves, do they have any awareness of the possibility of being hacked or attacked? Or do they think it's not important?

00:30:40 TPU5

For their own cybersecurity….

00:30:41 Interviewer

The general public, yes.

00:30:44 TPU5

The general public definitely doesn't have any awareness.

00:30:48 TPU5

They just need the internet be able to use, and that's it. And as for hacking, they probably don't know why they were hacked, so they can't do anything about it. There's still a long way to go for Taiwan's society to be aware of internet security. That's what I think.

00:31:11 Interviewer

So it might be necessary to set up some protective measures, but people might find it troublesome, won't they?

00:31:18 TPU5

Hmm. What protective measures are you referring to?

00:31:21 Interviewer

For example, just to prevent intrusion, maybe some websites will implement two-factor authentication or something, and people might find it annoying?

00:31:31 TPU5

The two-factor authentication on websites can also be bypassed.

00:31:35 Interviewer

What do you mean?

00:31:37 TPU5

It can also be bypassed, that's what I've been researching recently.

00:31:38 Interviewer

Oh, I see.

00:31:41 TPU5

Recently, that Bank SinoPac was hacked. It’s on the news so I am not afraid to talk about it.

00:31:47 Interviewer

Okay, okay.

00:31:50 TPU5

It was hacked, and then my boss asked me to study why Bank SinoPac was hacked. So I read some documents, watched some videos, and it turned out that they directly let you bypass the 2-factor authentication, so you can just swipe your card without it.

00:32:12 Interviewer

Is it like those no-card swiping methods?

00:32:16 TPU5

Different, different, it's different, it's actually sent to you, but they use social engineering or website vulnerabilities. For example, the issuing bank sends out an OTP code, but the hacker responds with an encoded version using a professional hacking tool to intercept and decode the packet. Then, when you respond to the intercepted packet, they can bypass it, use shifting or other techniques to decode it and obtain your OTP password.

00:32:49 Interviewer

I see.

00:32:59 TPU5

So, is verification safe? I don't think it's necessarily safe. But the general public is completely unaware of these things. They only know if there are viruses in your USB or computer? Will they be invaded? I think most people's general understanding is still at that level.

00:33:26 Interviewer

So, let’s move on to the ninth question, because as we just mentioned, the general public's awareness of network security is not very high. In this case, does the government have any plans to improve network security education?

00:33:40 TPU5

Now, the government can only improve the ability of those who are interested in information security. But for ordinary students, how do you educate the general public after they enter society? Advertisements? Promotional materials? Organizing activities and giving out prizes? These things are useless, because there are too many people and too many computers. How do you reach them? Education? Using Facebook and Google ads?

00:34:21 Interviewer

Hmm, using some social media platforms that people are more likely to see.

00:34:25 TPU5

Well, using LINE to promote it may be a direction. It’s just, people ususlly just ignore it after reading it. How do you get their attention?

00:34:37 Interviewer

Right, hmm, hmm, yes.

00:34:40 TPU5

Because it's not a personal pain yet, they don't feel that their personal information has been leaked. Or, they have not been scammed. Their personal information has not been scammed, they won't feel any pain. So, you can only try to plan as much as possible.

00:35:02 Interviewer

So, it may still be necessary for them to have their personal information stolen before they pay more attention?

00:35:06 TPU5

Yes, they will pay more attention only when it happens to them. Otherwise, they usually won't pay attention. Some companies have their own regulations.

00:35:17 Interviewer

So for the tenth question, it's about your understanding of the government's recruitment or training plans for cybersecurity personnel in schools or outside of schools. What do you think of these plans?

00:35:30 TPU5

For within schools, since I'm currently studying in graduate school, there are many CTF competitions held within schools, as well as the AIS program. The government also organizes the Golden Shield Award, and there's also the AIS Information Security Talent Cultivation Program for college students to participate in.

00:35:57 TPU5

For high schools, they also have the Golden Shield Award, but there's nothing for below high school, as they may not have learned basic subjects or be interested in learning about computers.

00:36:11 TPU5

As for cybersecurity personnel outside of schools, I haven't heard of any programs currently available.

00:36:28 Interviewer

I have seen that the government does publish some training programs online, and people can sign up for them, but I'm not sure how effective they are or if there is enough incentive?

00:36:41 TPU5

Are you referring to subsidies?

00:36:43 TPU5

Those are just for general information and technical skills.

00:36:47 Interviewer

Hmm, just basic knowledge?

00:36:50 TPU5

As far as I know, there doesn't seem to be any programs available for the general public to become cybersecurity professionals.

00:37:02 Interviewer

Right, so it's quite insufficient?

00:37:05 TPU5

Yes, but if you're talking about within schools or government agencies, then they all have their own training programs!

00:37:11 Interviewer

I see。

00:37:14 TPU5

Like us, we cultivate ourselves!

00:37:17 TPU5

Ah, we R&D personnel in the information department also cultivate ourselves. We are not quite like the public sector, you know? Because we are not IT personnel. I used to be one, but I was transferred here to work in information security.

00:37:36 Interviewer

OK, do you think the current training is sufficient?

00:37:45 TPU5

Definitely not enough, because as an IT personnel, you need a four-year university education foundation, and then you need to further cultivate in network security and information security. Usually, you will only get in touch with these after graduating from college.

00:38:05 TPU5

Look at the many university students, but there are very few information students who specialize in network security. Although the teachers are promoting it, they will say that information security will be in great demand in the future and that every industry will need it. But the truth is, in every industry, security personnel will only be regarded as IT personnel, and their salaries will be the same as those of others. However, they need to know more and understand more, but will the managers know this?

00:38:51 Interviewer

I see.

00:38:53 TPU5

If you work for a security company that specializes in hacking, then their training program will definitely be sufficient. They will also determine at the beginning at what level you should aim for, such as how high you should rank in CTF or Golden Shield Awards, or if you can earn a name in some foreign competition, etc.

00:39:28 TPU5

In other countries, or when looking at each department, such as the Ministry of Education or the Ministry of the Interior, IT personnel are almost all participating in CTF, attacking data, and how to do defense. They learn by doing. There is also a good suggestion, which is now available in Taiwan. If you discover a vulnerability in a website, either security personnel or security network, you can report it and upload information on how you discovered and invaded it. Then there is an organization, which sort of belongs to public sector, that will review it to see if it is valid. If it is indeed a vulnerability, the organization will inform the relevant authorities or the website operator about it. They will tell them If they do not update it, they will be the consequences, and the relevant authorities will reward the reporter.

00:40:46 Interviewer

The person who discovered it? This gives them an incentive.

00:40:47 TPU5

Yes, I think this plan is actually quite good. I believe we should increase the cooperation between academia, industry, and the public sector.

00:41:03 Interviewer:

Okay, yes, many are promoting this, academia, and the industry sectors.

00:41:08 TPU5

You see, if the industry provides a high amount of reward, and then you help me attack my website, once you find it, you will tell me, like Google, Google and Meta are doing this.

00:41:20 Interviewer:

Hmm.

## Section D

00:41:23 Interviewer:

Okay, then let's move on to the D section, which is the collaboration between the public and private sectors. The first question is, based on your understanding, what do you think about the collaboration between the public and private sectors in terms of network security? Does it really help the development of network security?

00:41:42 TPU5

It does help because we cannot learn everything about network and information security.

00:41:48 TPU5

Each area requires highly specialized professionals, such as Linux. You need to know about the specified vulnerabilities of Linux, for example.

00:42:05 Interviewer

I see.

00:42:07 TPU5

And, for each website, we cannot possibly know all the programming languages, such as PHP and ASP. If professionals from relevant fields can work together to investigate cases, it would be a good thing. We have an industry association that works with us in investigating cases. The chairman of the association, who is an expert in network security and packet filtering, helps us check for SQL injection instructions, malicious programs, and so on. Although we can look at them ourselves, it is always better to have experts to confirm what we say.

00:43:12 Interviewer:

Okay, got it.

00:43:14 Interviewer

Did you say he's a Taiwan Taiwan's director?

00:43:18 TPU5

Network Traffic Packets Analysis Association.

00:43:20 Interviewer

Packet Association, hmm.

00:43:21 TPU5

Packet.

00:43:27 TPU5

He will come to assist us, and if there are any issues with information, we can ask him.

00:43:35 Interviewer

How will you cooperate with him?

00:43:38 TPU5

What do you mean by cooperating?

00:43:40 Interviewer

What kind of assistance will he provide to you?

00:43:42 TPU5

No, it's just a word, "hey, come over here, don't come over there."

00:43:47 Interviewer

And then what will you do?

00:43:49 TPU5

Then we will show him the information, and we may need to do something here.

00:43:53 Interviewer

So he gives you advice?

00:43:55 TPU5

Yes, he will give us advice.

00:43:57 Interviewer

OK, I see.

00:44:00 Interviewer

So, for the second question, do you think there are any collaborations between public and private sectors in Taiwan regarding internet security?

00:44:11 TPU5

We have many collaborations between public and private sectors. The Criminal Investigation Bureau also has some hackers to help develop software.

00:44:17 Interviewer

I see.

00:44:19 TPU5

Like developing forensic software. Do you remember the hacker Chen Ing-hau or the CIH virus in 1998? He was a hacker and collaborated with the Criminal Investigation Bureau, so later on...

00:44:42 Interviewer

He was originally a bad hacker, right?

00:44:47 TPU5

Yes, he wrote a program that automatically shut down the computer after 60 seconds, I think. He was famous for that. You can search for Chen Ing-hau CIH on your own. He was a hacker who had a global impact, and he worked with the Criminal Investigation Bureau. Later, he started his own company.

00:45:19 Interviewer

Yeah, yeah, I know. It was a long time ago.

00:45:24 TPU5

Right.

00:45:26 Interviewer

So, what do you think of these collaborations? How do you think the current collaboration model works?

00:45:32 TPU5

Well, I think hackers are getting better and better. They can avoid some of the ways we track them on the internet, such as IP addresses. Nowadays, everyone uses Tor, which is a way to jump to another country before accessing the website they want to engage in malicious or threatening behavior. It is difficult to trace them in these cases, and international cooperation is required.

00:46:09 TPU5

The issue of our country's sovereignty or mutual judicial assistance is something we cannot solve.

00:46:22 Interviewer

Right, we cannot solve it. So, do you think that this kind of cooperation usually requires the help of hackers? Is that the case?

00:46:34 TPU5

Oh no, it doesn't have to be hackers. We need technical experts.

00:46:42 Interviewer

Do you think this kind of cooperation is possible? Which direction do you think it should develop in, in general?

00:47:03 TPU5

Actually, we can already trace IPs in Taipei City. If a company that has been hacked provides us with logs, we can trace them. But if the IP is foreign, we really can't do it. Even if it's a public-private sector cooperation, it is impossible to achieve unless it is a cross-border cooperation.

00:47:39 Interviewer

So, international cooperation may be necessary.

00:47:44 Interviewer

OK, but that's even harder.

00:47:45 TPU5

Hmm, it's even harder if it's from North Korea's IP. What if it's from China's IP?

00:47:51 Interviewer:

So, you don't want to touch it?

00:47:54 TPU5

Yes, it's really difficult to solve this part. Of course, when it comes to mutual improvement of professional knowledge in the domestic environment, I think it's still good.

00:48:10 Interviewer:

OK, then let's move on to the fifth question. Just now we talked about the overall situation in Taiwan. Do you have any cases of public-private sector cooperation here?

00:48:23 TPU5

Yes, we do. Our economic team cooperates with companies like [the name of a bank], and we have mutual cooperation in cases involving credit card fraud or warnings. We also cooperate with a certain company on investigating virtual currency, establishing a system for tracking and investigating virtual currency-related knowledge.

00:48:56 TPU5

These mechanisms, well, a few years ago when we still knew not much about the virtual currency, we didn't know what it was or what wallets were for. We were clueless about how criminals committed crimes and why we couldn't catch them.

00:49:25 TPU5

But now they not only cooperate with us to investigate, but also train a group of people to have knowledge on virtual currency. When it comes to virtual currency-related crimes, we also conduct searches and seize virtual currency transfers. It's all not a problem for us and it is definitely helpful.

00:49:50 Interviewer

Okay, so in that case, where do you think we can improve our collaboration in the future?

00:49:56 Interviewer

And that's it, I'm just here now.

00:49:59 TPU5

The sixth and the seventh questions?

00:50:01 Interviewer

Yes, because you just mentioned that these things are actually not bad in your opinion, because at least they have been established and there is mutual assistance. So, how do you think we can further collaborate in the future and do better?

00:50:16 TPU5

Collaboration between public and private sectors.

00:50:19 Interviewer

Based on what you just said, you could give more details about the collaborate with Fubon or cryptocurrency companies.

00:50:23 TPU5

Because it all depends on whether the private sector is willing to collaborate with the public sector, and they also need to spend extra time with the public sector. This is our job, investigating crimes is our job, and we need this knowledge. We need to know how to track channels, software, or methods, so if the private sector is willing to collaborate with us, we are certainly willing, but they actually don't have that much time to collaborate with us.

00:50:58 TPU5

Even if I tell you that many companies that have been hacked, we help them check, they are still very unwilling. It really depends on their willingness.

00:51:10 Interviewer

Their willingness.

00:51:11 TPU5

I think it all comes down to willingness.

00:51:16 Interviewer

So, does this mean we need to find a way to increase their willingness to cooperate?

00:51:21 TPU5

Yes, we need to find ways to increase their willingness. For example, when we cooperated with [the name of a bank] before, they held a press conference to enhance their corporate reputation and visibility. Actually, we don't need visibility, but they do. Fubon is a large corporation, and because the banking industry is highly competitive, we can tell them that cooperating with us will benefit them.

00:52:02 TPU5

But what about small and medium-sized enterprises? If we want to work with them, people might be concerned if their systems have any problems.

00:52:10 Interviewer

So, they care a lot about their reputation?

00:52:12 TPU5

Yes, they do.

00:52:13 Interviewer

So, if we want to cooperate with them, what should we do?

00:52:14 TPU5

They may not be willing to cooperate easily.

00:52:17 TPU5

When we ask them for logs, it's not easy to obtain them, and there are no rules requiring them to cooperate with us.

00:52:25 TPU5

In that case, we can only rely on Personal Information Protection Act. If there is a leak of personal data, and people are defrauded because of transaction records, a department that I forgot the name in the Ministry of Digital Affairs will impose penalties on enterprise. Otherwise, we will have no way to deal with them if they don't cooperate.

00:53:01 Interviewer

Okay, I think we've covered most of it.

00:53:07 Interviewer

Okay.