# Transcript

## Section A

00:00:01 Interviewer

Alright, next we're going to conduct an interview with TPU3.

00:00:06 Interviewer

Alright, let's get started. I'll begin with section A. So, the first question is, what type of organization does your unit belong to?

00:00:14 TPU3

The public sector. We're at the [a government criminal investigation unit], yes, the public sector.

00:00:17 Interviewer

[a government criminal investigation unit], got it. So, moving on to the second question, what is the name of your unit?

00:00:25 TPU3

I'm in the [a government criminal investigation unit].

00:00:30 Interviewer

OK.

00:00:31 Interviewer

And how long have you worked in this unit?

00:00:35 TPU3

About 5 years, almost 6.

00:00:38 Interviewer

Over 5 years.

00:00:39 Interviewer

Alright, the fourth question is, what is your job title in this unit?

00:00:43 TPU3

Uh, in terms of my position, I... in the earlier part, I was mainly involved in... currently, I am assigned to... I am currently working in the field operations of [a government criminal investigation unit]. We are considered an fieldwork unit within the investigative department. My role involves investigating various types of crimes, including cyber crimes and other criminal cases. Oh, and before last year, I was a staff officer in our business unit, where I was in charge of building and maintaining criminal investigation-related databases for the [the name of a municipal police department].

00:00:57 Interviewer

OK.

00:01:16 Interviewer

Moving on to the fifth question, what are your main responsibilities?

00:01:21 TPU3

In terms of responsibilities, I am currently assigned to fieldwork. We have four teams in our unit, and I lead one of the fieldwork teams.

00:01:32 Interviewer

When you are leading your squad, your mainly job is investigating criminal cases?

00:01:39 TPU3

We investigate various types of criminal cases. This includes cyber crimes, and recently, we've had some sensitive cases that are related to information security. If there are related agencies reporting cases, we'll try our best to investigate. So, our main responsibility is investigating all types of criminal cases, without any specific limits.

00:01:54 Interviewer

OK.

## Section B

00:01:57 Interviewer

Okay, let's move on to Part B. The first question I have is about your opinion on what the main types of network attacks Taiwan are currently facing, and what methods are being used in these attacks. Could you provide some examples?

00:02:13 TPU3

Well, in terms of network attacks, I think there are quite a few cases where they... Like some of the cases we encountered recently, they targeted certain organizations, such as running associations, some prominent government departments or judicial personnel departments, and launched some DDOS attacks that paralyzed their websites. Also, there are some attacks that steal personal information. And there are some other types of attacks, such as... When you say "network attacks," what exactly are you referring to? Because network attacks are actually quite broad. Is there any specific type that you are interested in?

00:02:50 Interviewer

I didn't specifically limit it to anything, just overall.

00:02:53 TPU3

Does cybercrime count? Or...

00:02:55 Interviewer

Yes, cybercrime also counts.

00:02:56 TPU3

That's too broad then, because cybercrime includes various types of criminal cases we are currently investigating, such as fraud, gambling, and drug trafficking, all of which are related to the internet. With the development of mobile phones, many cases of online defamation and threats are also on the rise. And these kinds of cases are the most we have encountered so far. If the scope is that broad, then actually, from the past to the present, especially since the second half of last year, we have encountered a lot of cyber threats against the public, such as bomb threats sent to the Presidential Office mailbox or some government department mailboxes. These types of threats are very common.

00:03:23 Interviewer

I see.

00:03:31 Interviewer

OK, it seems like I forgot how long ago, it should be last year when there was, that is, the Interviewernese cyber army, and then, it was during the election... during the election, and then there were on the railway and other billboards or something, did you encounter that?

00:03:46 TPU3

We have heard that, but we did not get involved because, to put it this way, for those types of attacks that are more related to the other side of the strait (China), if it comes over, actually, it will still be divided, like those major agencies, like the railway, usually this type of cases often go to the Investigation Bureau.

00:04:05 TPU3

Yes, we will know about it here, and each unit will try to find ways to help, for example, to contact the railway bureau if they need any help. They usually say that they have already gone to the Investigation Bureau or they have their own information security department to do preliminary handling, yes.

00:04:20 Interviewer

OK, I see.

00:04:22 Interviewer

Then we move on to the second question. The second question is, what do you think is the main target of cyber attacks in Taiwan? And also?

00:04:30 TPU3

Well, I think there are probably a few major ones, like, uh, the MRT, and then the stations, yes, and the Presidential Palace, yes, and then some...there is also the Chiang Kai-shek Memorial Hall, yes, so these are some of the significant facilities. And also some of Taiwan's well-known landmarks, like Taipei 101, yes. And then some of the important transportation, such as Taipei Station, some major MRT stations and transfer stations, yes, have received some threats like placing bombs.

00:05:03 Interviewer

It may be the government or some large transportation?

00:05:11 TPU3

Yes, or some high-profile landmarks, yes.

00:05:13 Interviewer

I see. High-profile landmarks.

00:05:15 Interviewer

Do you have anything special... besides what you just mentioned, is there any industry that is particularly vulnerable to attacks?

00:05:24 TPU3

Oh, there is a special industry that I have encountered before, in that... it's not really an attack, but their personal information was stolen... stolen... stolen, that's the Taiwan Road Running Association.

00:05:33 Interviewer

Oh, the Taiwan Road Running Association.

00:05:34 TPU3

Yes, the running association is quite special, eh, how could they be stolen... maybe because in Taiwan, I think that in recent years, the sports trend has been on the rise, so there may be more personal information in it, and then such a case happened.

00:05:49 Interviewer

OK, then let’s go to the third question, what do you think are the factors that affect Taiwan's network security?

00:05:58 TPU3

I think that most recently, because as I just said, we started receiving many cases of bomb threats in the second half of last year, then...

00:06:08 TPU3

Actually, many of them, I think that Taiwan's departments, because we are too... should say that many of our types of network attacks, they first have to find, this is it, they must first find a channel to get into, for example, today I want to leave a threatening message, I want to spread the threatening message, there must have to be a place for me to get in, oh, for example, I search for the mailbox of the Presidential Office, okay, now actually all the major leaders or major agencies, they all have some... that is, channels for the public to express their opinions.

00:06:24 Interviewer

Hmm.

00:06:39 TPU3

Actually, many people use this method to enter. When they leave a message, Taiwan doesn't have... doesn't have those so-called 2-factor authentication mechanisms. This means that anyone can search on Google for something like the Presidential Office of the Republic of China or the Executive Yuan or the Judicial Yuan, and they will find mailboxes where they can express their opinions. They can even do it anonymously. Because you need to enter your basic information when you leave a message, and this information has not been verified, anyone can impersonate anyone else...

00:07:01 Interviewer

I see.

00:07:15 TPU3

And then they can leave threatening messages, and... Basically, when such a message is sent, the relevant departments become nervous and feel the need to pass it down for us to investigate. I think there should be some sort of double authentication process. For example, when you want to send comments to the mailbox today, I may need to authenticate your email and verification code, and then verify it through your phone number. This way, it may be easier to prevent this kind of thing. Because now, I encounter many cases where someone leaves a message, and actually, the information that person leaves are….. For example, if I want to leave a message to the president’s mailbox, I need to specify who I am and leave my contact number. But the contact number doesn’t need to be verified, I could leave a fake number on purpose. For example, I leave a phone number, but it's clearly another department's phone number that I can find on Google. This kind of situation happens a lot. So I think the main problem is with the internet. Even the government doesn't have the awareness to prevent it. I think it's not good enough... People might think that this is a channel for collecting public opinions, but in fact, it is being used by criminals.

00:08:18 Interviewer

So basically, you think that in terms of prevention, it's not yet very thorough, so there may be some loopholes?

00:08:26 TPU3

Yes, there's not much caution.

00:08:31 Interviewer

Okay, so do you think there are other factors besides what you just mentioned, such as social factors or political factors? For example, someone need money or….maybe some political influences.

00:08:57 TPU3

I think political factors are definitely the reasons, especially when we think about our relationship with the other side of the strait (China), which has become increasingly tense in recent years. Yes, actually... it's quite evident that when we have conflicts with them, during tense situations, we can clearly feel an increase in cases related to cyber threats or intimidation on the internet.

00:09:28 TPU3

So I do think there is some impact.

00:09:30 Interviewer

Okay.

00:09:32 Interviewer

Can you trace these incidents back to their source on the other side of the strait (China)?

00:09:37 TPU3

There was a case of stolen information where someone impersonated our former mayor on LINE and requested information from other departments, schools, etc., saying he was the mayor. Some departments were suspicious and didn't give information. I am not sure if some department did give him the information. Later, it was discovered that the person impersonating the mayor was actually from the other side of the strait (China). We investigated and found out that he was likely a member of a cyber army or using a jump server company, but we couldn't continue our investigation once it reached the other side of the strait.

00:10:34 Interviewer

I see.

00:10:35 TPU3

We can only confirm that… because the relevant registration data has come back, and it is confirmed that it is in China. That's how it is for this particular case. As for the other cases, I can say that from the end of last year until now, we have investigated cases involving threats to set off bombs or threats to kill someone, similar to that. And the sources of these cases, as determined in the end, are mostly from one or two individuals, and it has been confirmed that they are also from…. across the strait (China).

00:10:58 Interviewer

Okay.

00:10:59 TPU3

Yes, it could be the previous Chinese students who studied in Taiwan, and the students later went back to China.

00:11:03 Interviewer

Okay.

00:11:06 Interviewer

I have heard of a case before, last year it was also a Chinese student, and he also done similar crime in Singapore or...

00:11:15 TPU3

I'm not sure if he went to Singapore, but I know he is not within our jurisdiction now...

00:11:18 Interviewer

And then he went back, and there was no way to trace him?

00:11:20 TPU3

Right, he cannot be traced. And he is still doing these things overseas, like threatening to kill someone, kill Tsai Ing-wen, kill Su Tseng-chang, and threatening to detonate bombs, there are a lot of them coming in.

00:11:30 Interviewer

Okay.

00:11:30 TPU3

Yes, that's right. Going back to what I said before, our website and such things don’t have double authentication. For example, for the MRT, they have received too many of them, and every time they receive them, they have to forward them to the police to handle them. So we had a meeting with them earlier, and suggested that they introduce a two-factor authentication mechanism. That is, before you leave a message, you must verify through email and the phone number. They seem to have already introduced it, and it is indeed found that there are fewer of these messages after the introduction.

00:11:51 Interviewer

Okay.

00:11:59 Interviewer

Right, I remember now. It's like he had something to do with the railways in Japan.

00:12:04 TPU3

Oh, right, right, right, right, right, in Tokyo. And you see Japan is making a big move, and we are already a bit tired, but it is actually very dangerous because if there is a copycat criminal, he may not be him, he may be imitating him, and if he really does these things, I think if the vigilance of the police is reduced, then it is still quite dangerous.

## Section C

00:12:21 Interviewer

Alright, let's move on to the next section, the C section.

00:12:29 Interviewer

So for the C section, let's start with the first question. Based on your understanding, in what areas do you think the Taiwanese government's overall cybersecurity plan is focused on? And what do you think of these plans? Are they good or do they need improvement?

00:12:47 TPU3

Hmm, this one is a bit difficult for me personally.

00:12:49 Interviewer

It's okay, just share what you know.

00:12:50 TPU3

Well, I think that in recent years, we've seen the establishment of Ministry of Digital Affairs...

00:12:56 Interviewer

Yes, that's right.

00:12:56 TPU3

Oh, and some of the previously separate units related to information security that may have been under other old departments have been elevated in terms of their level, oh, so they've probably used the Ministry of Digital Affairs to integrate them across departments, and it seems like the government is targeting this area and trying to improve the overall level of cybersecurity.

00:13:17 TPU3

Yes, and in addition to that, based on our previous experiences in business operations or encountering situations, we have indeed noticed that they are indeed targeting cybersecurity. Especially in recent years, as we are a criminal investigation unit, we have the police department overseeing us. The police department regularly conducts vulnerability scans. Because as I just mentioned, my previous job involved managing our own criminal database, which is a system that allows colleagues to conduct data queries. Since it involves a system, it falls under the management of the information unit. So, we can clearly feel that in the past couple of years, there has been a significant focus on cybersecurity investigations, including regular vulnerability scans.

00:13:56 Interviewer

Okay.

00:13:57 TPU3:

Oh, right. The frequency has been increased, and there are levels, such as every six months, or sometimes there will be audits conducted by the city government.

00:14:01 TPU3

Well, I was just wondering if your cybersecurity is well-established. Implementing measures like the Government Configuration Baseline (GCB) can provide a clear sense of enhanced system security. I think it's a good practice to strengthen security in this aspect.

00:14:15 TPU3

However, relatively speaking, it may, um, how should I put it... feel like it's still in the early stages, like it hasn't really reached the deep level yet. Because a lot of times, when we investigate your network and system security, we are only asked to fill out things like forms and sent back. That’s it. So, it's still under observation, because after all, the Ministry of Digital Affairs was only recently established. I am happy to see it succeed, though.

00:14:47 Interviewer:

I suppose it was established last year, so it’s been a year?

00:14:51 TPU3

Yes, it was established around that time. But from the time of its establishment until now, although I felt that there was indeed a requirement to enhance overall information security as I mentioned earlier, I personally haven't seen much effect in practical terms.

00:15:08 Interviewer

I see.

00:15:11 Interviewer

Okay, because the first question was more of an overall cyber security, let's move on to the second question. The second question is, what do you think the current strategies of preventing online threats are? What are these strategies like? And then, how do you evaluate these strategies? I think questions two and three can be answered together. That is, do you think there are any ways these strategies can be improved?

00:15:48 TPU3

Can you give an example of what you mean by prevention strategies?

00:15:53 Interviewer

For example, if you are currently investigating a case, then usually, you will have a prevention strategy because of the occurrence of that case. You will review what happened and think about how to prevent similar cases from happening in the future. Or you might become aware of certain techniques, so you might make changes to your prevention strategies to address them.

00:16:20 TPU3

Well, currently, we do this regularly because sometimes we know about cases where personal information is leaked. It's not limited to government agencies, but also includes private entities like online shopping platforms, malls, and so on. These kinds of data leaks happen quite frequently.

00:16:47 TPU3

Oh, regarding data leaks, if it happens, the central government, possibly the Criminal Investigation Bureau, will handle it, and we will dispatch personnel to the scene. We have a standard form for checking each piece of leaked data, and we will ask the company about their leaked data because these cases usually lead to fraud. Because of incidents involving the leakage of personal information and subsequent fraud cases reported by the public, we investigate and identify which companies or which stages of the process had errors in handling personal data. We conduct checks in collaboration with their internal security personnel, gather relevant data, and then? Currently, we typically report to the central authorities, but it seems that our approach is more focused on handling individual cases rather than having a unified and standardized procedure. It's more of a case-by-case basis rather than a comprehensive approach.

00:17:48 TPU3

Yes, in terms of prevention strategies, I think we need to focus on the security of our network infrastructure. This applies to all industries and government agencies. The security of the networks must be a priority, especially for private businesses. It seems that it is necessary for our government to create a unified approach, but it is difficult to impose requirements on private companies. Regarding how to legislate on this issue, I think this is also a place to consider.

00:18:29 Interviewer

That's difficult.

00:18:30 TPU3

Yes, it's very difficult.

00:18:32 Interviewer

Okay, so we're moving on to the fourth question. Since we were just discussing prevention, the fourth and fifth questions can be answered together. The fourth question is about what strategies you know for responding to a cyber attack when it happens.

00:18:49 TPU3

Are you asking about what to do after or during the attack?

00:18:51 Interviewer

Yes, during the attack.

00:18:52 TPU3

During the attack, we usually... the first thing to do is to find a way to block it. As far as I know, we first need to block it and pause the damage, such as by temporarily shutting down the server if the website is paralyzed. Then we will investigate where the attack came from.

00:19:14 TPU3

Then we can further focus on, for example,…..I am not familiar with the details of this part……if they came in through a vulnerability in A, we can patch that vulnerability and look for any other vulnerabilities that need to be addressed.

00:19:26 Interviewer

I see.

00:19:27 TPU3

This is for a single part. However, as I mentioned earlier, because we lack a broader perspective, it's possible that other companies have experienced similar attacks. So if we can integrate these things, then A company's attack may not happen to B company, and I think this can be a more effective way to respond.

00:19:43 Interviewer

Mm-hmm, OK, so this also answers the question, which is that you….., so it's like, if there can be some integration, then it might be more efficient, right?

00:19:54 TPU3

Yes, yes, exactly. If there's a department or a mechanism that can do something like that, because I believe there are definitely a lot of things happening now. Well, actually, network attacks are very extensive, not just personal information, or paralyzed web pages. Sometimes they come in and take out your data, then go to you for extortion, encrypted extortion. In other words, they say, "Hey, you have to give me this much money, otherwise I'll put your information up for sale on the Internet."

00:20:20 TPU3

Many cases are like this, and because of reputation issues, these companies sometimes don't even report it. Yes, some do report it, but sometimes it's difficult to deal with because these hackers, these network attackers, when they come in, they leave a backdoor that you can't track. Sometimes they even put data for sale on the dark web, making tracking very difficult. So we can only deal with it case by case, such as targeting this company. Our usual approach is to teach them how to negotiate with the other party and try to minimize the damage. Of course, we also need to understand how they came in, but usually this information is one by one... one by one... one by one. Yes, so maybe you will find that these hackers, the same group of hackers, probably use the same method. But because companies don't communicate with each other or do horizontal integration, you... if there is a mutual communication, and company A suffers attacks, we will have a mechanism to let everyone know that... actually, there have been such... a case of a network attack and stealing personal information, and they did it in some sort of ways, so please check and strengthen it.

00:21:29 Interviewer

OK.

00:21:30 Interviewer

So, moving on to question six. Question six and seven can be answered together. As we talked about during the attack, there will be some measures for review and reflection after the attack. What do you think about your current review measures?

00:21:48 TPU3

Well, speaking from our own team's perspective, because our level is not as high as the central government. So usually, in our team, all of us are aware of the cases that occur. Therefore, if there is a network attack or data breach incident, colleagues within our team, through our team group or regular discussions, are generally informed about it. We have discussions that touch upon the knowledge of current techniques and methods used in such incidents.

00:22:18 TPU3

If there are any news reports about new emerging scam techniques or methods used in network attacks, we usually inform our colleagues, so everyone is aware. After being informed, it becomes clearer for individuals, whether it's their personal computers or encountering situations outside, such as when we conduct on-site operations. Sometimes, when we come across the suspect's or victim's computer, we can get a sense of the potential vulnerabilities and how they may have been exploited. This understanding is gained through discussions and sharing within our team. However, it's important to note that while we can understand how things are done during the investigation, we may not always be able to proactively prevent such incidents.

00:22:51 Interviewer

I see.

00:23:04 Interviewer

So, in terms of preventing these incidents, what do you think can be done to improve the situation?

00:23:13 TPU3

Well, I think we need to have a mechanism, yes, a mechanism or a...

00:23:18 Interviewer

A systematic one?

00:23:19 TPU3

Yes, a systematic one, a connected one. One aspect is to have a reporting system, a... a... a... well, how do I put it... a measure or a channel, that allows us to target all these incidents that occur on the front line, whether they are civilian or public. It can allow us to report these incidents upward, and then the relevant authorities can compile them to see exactly what types of cyber attacks have occurred on the front line, whether they are on the government or civilian sector, and what patterns of the attacks. Only then can we have a better way to prevent them, I think!

00:24:01 Interviewer

Alright, let's move on to the 8th question. So, what do you think about the general public's awareness of internet security?

00:24:11 TPU3

I think it depends on age group. The younger generation is more likely to be aware of not clicking on unknown links, how to avoid personal computer data leaks or theft, and how to prevent intrusion of malware. However, some of the older generation, who may not be as proficient in using mobile phones, are more likely to download unknown links or click on unknown webpages, which can lead to data leaks or theft of personal information.

00:24:57 TPU3

So, I think it's half and half in terms of general awareness.

00:25:02 Interviewer

Yes, it depends on age group. It seems that the older generation is less knowledgeable about internet security?

00:25:09 TPU3

Yes, they are less aware of cybersecurity.

00:25:15 Interviewer

Okay, so let's move on to the 9th question. Since we just talked about the general public's awareness, do you think the government has any specific plans to enhance awareness of internet security through education?

00:25:29 TPU3

Well, what I see is mainly focused on... currently, it's focused on things that have already happened, such as I think it's network security... cyber security, or some crimes caused by cyber security issues. The government is indeed strengthening this area, such as fraud, for example, if you see something on the internet, don't buy something with an unknown origin. Similar to this, I think I have seen that they are doing a lot of promotion in this area, whether it's on TV ads or posters that we see, which are government propaganda. But when it comes to the first level of prevention, how can you avoid your personal information from being obtained by scammers? Because most scams are like this, they have to find a way to obtain the victim's information first.

00:26:16 Interviewer

I see.

00:26:17 TPU3

Yes, then I can use that to scam them. Actually, I think the first-line prevention in this area... hasn't been seen much, right, right, I am not sure if the government… if the Ministry of Education has included the first line cyber security in the education, such as incorporating it into textbooks for national education, or….., but in our field, I haven't seen it.

00:26:33 Interviewer

I see.

00:26:35 Interviewer

Maybe there is only promotion, such as on the government website?

00:26:39 TPU3

Yes, but the effect of website promotion is not high, I think, because usually when I go to this website, I must have a specific purpose. I won't specifically go to see that thing.

00:26:46 TPU3

Yes, there are some, such as a warning popping up when transferring money from a bank, but it's not that... impactful, I think, yes.

00:26:57 Interviewer

Understood.

00:27:00 Interviewer

Or some multimedia. But for some online advertisements or ads in general, it seems like the older people may not necessarily see them.

00:27:09 TPU3

Yes, because I think most people are emotional creatures, so most people must have a sense of feeling, or you clearly feel pain, or feel fear, or have this kind of thing, you will be more focused on this area, usually it must be a crime case, or a large number of such crimes have occurred, then you, such as someone around you being deceived, someone being cheated, then you will be more vigilant, yes, usually when you are surfing on your phone, or when you are doing some activities related to the internet, I think... the security awareness in this area is really lacking in education, and the criminals are very aware of it.

00:27:46 TPU3

Yes, that's right. They are more aware because they know that, for example, we also use these related technologies, such as the internet and social engineering, to find ways to identify and locate individuals during the investigation process. However, we also try to create some things that can entice them to click on, and they are very vigilant against things like that.

00:28:18 TPU3

Sometimes they won't fall into traps, and they know that the police are fishing or doing something like this, yes, so sometimes they are more aware than we are, and we ourselves are not aware of that.

00:28:27 Interviewer

Okay.

00:28:29 Interviewer

So, let's move on to the tenth question. What do you think the government's plans are for cultivating cybersecurity talents, both within and outside of schools? Have you heard anything about this? What do you think about these plans?

00:28:46 TPU3

I'm not really sure about this. I'm not sure if the government has any plans specifically for this, but they should, since they established the Ministry of Digital Affairs last year. As far as I can recall, the Cybersecurity Management Act was also revised, and because of this and recent amendments to the law, I've heard that every bank is required to have a cybersecurity department or officer.

00:29:03 Interviewer

I see.

00:29:16 TPU3

Yes, that's the regulation. Since banks deal with people's assets, they have the highest standards to meet, and as a result, they attract talent in this field. They are also looking to recruit individuals with a information technology background in law enforcement to join their system. As for specific plans like offering courses or credit classes to cultivate talent in this field, I'm not really sure. I don't know if they have anything like that, but at least it seems like they are trying to establish a system based on laws and regulations.

00:29:59 Interviewer

I saw on the government's website that they have some courses, but I don't know how effective they are or how they are implemented.

00:30:07 TPU3

Yes, because you need to have incentives to attend such courses, otherwise who would come? Typically, people with a background in computer science would go to information technology companies, even TSMC, or other large companies where they can get higher salaries. Yes, if you establish specialized training programs for nurturing talent in the field of cybersecurity, once they complete their training and graduate, where would they go? If they are only considering government agency jobs, the incentives may not be as enticing for them.

00:30:32 TPU3

Yes, so I think that...if the aim of the training program is to cultivate individuals with expertise in cybersecurity, it would be beneficial if they could leverage that expertise to secure positions in prominent companies. However, it would be essential for them to join the cybersecurity departments of these companies. I agree that this would be a positive outcome.

00:30:48 Interviewer

Hmm, mainly in terms of incentives?

00:30:48 TPU3

Yes, they need incentives, otherwise it won't attract enough talented people.

## Section D

00:30:58 Interviewer

So now we're moving on to the section D. We are going to talk about the cooperation between the public and private sectors, and for the first question... it's about your own opinion on the concept of the public and private sectors working together on cybersecurity. What do you think about this idea?

00:31:15 TPU3

I think it's definitely a good thing. I strongly support this because even though we work in the government sector... we're still just a small group in society as a whole.

00:31:32 TPU3

It's a bit like in the process of criminal investigation, even though we can access surveillance footage, there's often a lot of information that we need to obtain through cooperation with the private sector. So for cybersecurity, it's definitely necessary to have this kind of cooperation, especially since all of our telecommunications are now handled by private companies like Chunghwa, Far EasTone, and Taiwan Mobile. We must work with them in order to enhance the overall balance and fairness of our cybersecurity measures.

00:32:03 Interviewer

OK.

00:32:05 Interviewer:

So let's move on to the second question. I think questions 2, 3, and 4 can be answered together. Based on your understanding, how is the collaborate mode between the public and private sectors in Taiwan currently, and what are some examples or experiences you can share?

00:32:26 TPU3

Well, I'll give two examples. The first one is related to the subway system, which we mentioned earlier. Is the subway system run by the private or public sector?

00:32:39 Interviewer

It's hard to define. Is it currently private?

00:32:47 TPU3

I think it's private now, right? I remember it changed.

00:32:50 TPU3

Yes, it's like what we talked about earlier with the subway incidents where people threatened to bomb the subway. Back then, we have contacted the high-level officials in charge of the subway directly. When these incidents happen frequently, they will feel inconvenient, annoyed, and painful, and then they will be more willing to cooperate with the police. At that time, we discussed with them whether we should hold a meeting to discuss how to avoid such situations. Finally, they introduced the mechanism of dual authentication that we just mentioned. As for the second part, it is about incidents where personal information leaks occur frequently in online shopping platforms like Kingstone Bookstore, Shopee, and Ruten. We also discuss with them on the front line. However, I feel that this cooperation is not as effective because when we discuss with them, they just cooperate by filling out some information and then it ends there. Unfortunately, there are certain companies that have been experiencing data breaches from a few years ago until now.

00:33:59 TPU3

Yes, that's right. It means that they haven't really made any big changes of it. In this regard, it is necessary to rely on legislation to require them to take actions or to provide sufficient incentives for them. Because, for them, it can be an uphill battle with little recognition. They may question why they should invest so much effort into it. Improving cybersecurity involves conducting inspections and replacing infrastructure throughout the entire network architecture, which can be a significant cost in terms of finances, manpower, and other resources.

00:34:24 Interviewer

Hmm.

00:34:26 TPU3

They may be unwilling to undertake such tasks, and we cannot force them to do so. Therefore, in this regard, it depends on their willingness. Currently, the cooperation mechanisms are mostly limited to individual cases, focusing on a case-by-case basis.

00:34:39 Interviewer

Okay, so besides the examples you just mentioned like Shopee and Kingstone Bookstore, do you have any partnerships with companies that specialize in technology or internet security, like private companies?

00:35:04 TPU3

They have their own relevant departments.

00:35:05 Interviewer

They have their own relevant departments?

00:35:06 TPU3

Yes, we go to the scene and try to understand where exactly the system or process went wrong, leading to continuous data breaches. We gather information and they assign relevant personnel to communicate with us. We have a form that they fill out and provide us with the necessary details. However, this cooperation is limited to that extent. If they persistently ignore our advice or continue to cause data breaches resulting in fraud, our last resort is to request penalties from the regulatory authorities in charge of their respective industries. But even then, the penalties imposed may not always be severe, which may not serve as a strong deterrent for them.

00:35:47 Interviewer

Okay.

00:35:48 Interviewer

So, in that case, what difficulties do you think there are in terms of cooperation? Although you mentioned it briefly earlier, where do you think the main difficulties lie?

00:35:58 TPU3

I think the main difficulty lies in the fact that we do not have, because I think if you want to use incentives or provide incentives to encourage them to improve this area, it's difficult to do so. Instead, the difficulty lies in the fact that there is no effective legislation to require them to do a good job in network security. For example, a large company has too many network services. It can be accessed through various apps, and if this area of security is not done well, it can cause a lot of risk.

00:36:26 Interviewer

I see.

00:36:33 TPU3

Oh, so actually there is not an effective law or regulation that requires them to do this. If they violate it, are there any penalties? And such penalties must make them feel the pain, otherwise it's useless. It must be done.

00:36:47 TPU3

Yes, this area is very lacking.

00:36:48 Interviewer

Okay, so let's move on to the fifth question. The fifth question is about whether your unit currently has any modes or experiences of collaborating with the private sector, given that you just talked about understanding the current mechanisms of public-private cooperation in Taiwan.

00:37:10 TPU3

Our current mode of collaboration and experience is primarily focused on individual cases, as we are a criminal investigation department. For example, in most cases, we work together when investigating incidents. Sometimes, we encounter situations where certain companies frequently experience data theft or leaks, and they reach out to us for assistance. Over time, we have established a communication channel for such cases. However, our interactions are primarily case-specific. We rarely discuss how to strengthen cooperation. We may identify possible loopholes and tell them. But we do not have a well-defined mechanism for that, and most discussions revolve around addressing specific cases.

00:38:03 Interviewer

So it's all on a case-by-case basis?

00:38:05 TPU3

Yes, that's correct.

00:38:07 Interviewer

Okay, so, the sixth and seventh questions may have been touched upon earlier, so in your opinion, what aspects can be improved in such mechanisms? Since... there isn't a definite mechanism, and it's all done on a case-by-case basis.

00:38:26 TPU3

I think it's possible, I think it can be done in parallel.

00:38:29 TPU3

For example, your company often experiences incidents such as data theft or breaches that lead to network attacks and subsequent cases. In such instances, our collaboration can primarily focus on addressing the specific case at hand. In the meantime, however, I believe it would be beneficial to involve the information department from our side and the network management department from your side in the discussions. After handling the immediate case, we can gather relevant information and engage both departments in a conversation about how to improve and patch the identified vulnerabilities. I feel that, since an incident has already occurred and caused inconvenience and damage to both parties, they may be more willing to participate in the subsequent work and take necessary measures for improvement.

00:39:28 Interviewer

Okay, great. So, my last question is about whether you have experience collaborating with technology professionals who work for private companies. I understand that such collaborations may have some difficulties, such as needing to request data from companies like Chunghwa Telecom, and the investigation may need to be conducted in secrecy, so you need to avoid sharing too much information with them.

00:40:17 TPU3

Yes, so basically, we just tell them that we are exchanging data with them, and we won't tell them too much. Yes, they all know that. Usually, they will cooperate because there are many similar cases happening. They are also willing to help find a solution because, after all, such incidents damage their reputation as well. So, they are willing to cooperate and help us handle the case. Usually, when we handle these cases and work together with their company, we can solve the problem of data leaks and subsequent fraud cases. We catch the perpetrator, but the victim is still within their company. So we need to figure out how to prevent these data leaks from happening again because there will be a second, third, or fourth perpetrator. If we only rely on our own strength, we can only target specific cases. Therefore, cooperation with relevant departments is necessary to truly reduce the occurrence of cybercrime and increase online security.

00:41:13 TPU3

They are willing to cooperate, but the key is still how to prevent themselves from…. Yes, this is the key...

00:41:20 TPU3

I think that only relying on our own strength may only work on specific cases. It is still necessary to cooperate with relevant departments in order to truly reduce the occurrence of cybercrime and increase online security.

00:41:37 Interviewer

Hmm, okay.

00:41:41 Interviewer

Then I think we can end it here. Thank you.

00:41:44 TPU3

Okay, good.

00:41:47 TPU3

Okay, thank you.