# Transcript

## Section A

00:00:00 Interviewer

Now we will begin the interview with TPU2. First, I will start with Section A, which covers basic information. The answer to the first question is that you work in the public sector. For the second part, please briefly introduce your unit.

00:00:24 TPU2

I currently serve in the [a national criminal investigation agency].

00:00:29 Interviewer

OK, the [a national criminal investigation agency]. How long have you been working in this unit?

00:00:33 TPU2

I've been with the [a national criminal investigation agency]for six years.

00:00:36 Interviewer

You've been with the [a national criminal investigation agency] for six years?

00:00:37 TPU2

Yes, six years.

00:00:38 Interviewer

OK, and what is your current position?

00:00:40 TPU2

My primary duty is criminal investigation.

00:00:44 Interviewer

Criminal investigation. What are your responsibilities?

00:00:47 TPU2

Currently, as a telecommunications police officer, my work includes not only investigating crimes related to network attacks, but also other criminal cases such as fraud groups, drugs, violent crimes, and the crackdown on illegal firearms and ammunition. Major cases are also included.

00:01:17 Interviewer

OK, got it.

## Section B

00:01:18 Interviewer

Okay, now let's move on to Part B, which is about network security. So, for the first question, based on your experience and perspective, what do you think are the main internet attacks Taiwan is currently facing? Also, what are the methods used by attackers, and can you provide examples?

00:01:38 TPU2

Generally, the cases we handle involving network attacks are mostly from civilians, such as individuals and private companies. For example, a company's data may be hacked and stolen by hackers. One example is the case of YouBike and iRent (a Taiwanese car rental company), where their data was allegedly stolen. But this is just an example.

00:02:15 Interviewer

I see.

00:02:16 TPU2

There are also some private companies that may be invaded by hackers, and their data is locked up by a Trojan horse. They may be blackmailed for ransom. Some hackers may also invade and steal customer data, and engage in other criminal activities such as fraud against victims. For individuals, the attacks mainly involve hackers breaking in and tampering with data, using the victim's network information through their platform to alter other people's data, or launching anonymous attacks, and so on. These all exist. Like the case last week, where a hacker used a restaurant's network to infiltrate a company and engage in hacker activities, altering and deleting important data, causing great losses and harm to the company. So sometimes the types of cases are quite diverse, but they mostly involve companies and individuals.

00:04:19 Interviewer

Companies and individuals?

00:04:20 TPU2

Yes, and public sectors are actually relatively rare.

00:04:24 Interviewer

Public sectors are relatively rare?

00:04:26 TPU2

Yes, public sectors are relatively rare, except for the case last time where suspected online army attacked some government agencies and posted images of the Chinese five-star flag. You may have seen that news. That kind of attack is relatively rare.

00:04:44 Interviewer

I see. But such incidents get more attention every time they happen, right?

00:04:48 TPU2

It's more shocking because it's the five-star flag.

00:04:51 TPU2

Hmm, there is a special purpose for that. Like some of those tracking activities, the IP addresses all come from the other side of the strait, so that's more special.

00:05:04 Interviewer

Hmm.

00:05:06 Interviewer

So mostly it's individuals and some private enterprises?

00:05:11 TPU2

Yes, mostly private enterprises.

00:05:12 Interviewer

But fewer attacks on the government?

00:05:14 TPU2

Yes, fewer attacks on the government because the government's firewall may be better or more effective.

00:05:25 Interviewer

Hmm, but if it's an attack between countries, it could be strong, but does Taiwan have that kind of attack?

00:05:35 TPU2

Yes.

00:05:37 Interviewer

Has Taiwan encountered that kind of attack before?

00:05:43 TPU2

Uh, it's hard to determine if it's between countries. Sometimes...

00:05:46 Interviewer

Right, but you just mentioned that those online army could be?

00:05:47 TPU2

Yes, that's right. Those are some enthusiasts who are young and thinking it would be cool to invade others. Like that company in the United States that was hacked before, and then they would mark something to prove that they had infiltrated them. Taiwan had some young hackers before who were quite skilled. He went to a very important foreign website and marked it to prove that he had penetrated it.

00:06:23 Interviewer

Hmm.

00:06:31 Interviewer

Understood. That proves that they are very skilled and they want to prove their abilities?

00:06:35 TPU2

Yes, that's right. Some young people like to show off like that.

00:06:42 Interviewer

Alright, then let's move on to the second question. What do you think is the main target of cyber attacks in Taiwan currently? And what are the reasons behind it?

00:06:56 TPU2

Well, I think there are two types. One is to steal data, oh, and the other is for hackers to lock up their data and then demand a ransom. And then there's another type, which is revenge or retaliation, possibly from a former employee or some other kind of business dispute. So, basically, it's like that.

00:07:26 Interviewer

Okay, I see. Do you think there are any specific industries that are more likely to be targeted?

00:07:38 TPU2

I think there are quite a lot in private companies because their firewall may not be that strong or something like that. So, we often get more requests for help from private companies.

00:07:51 Interviewer

I see. Alright, let's move on to the third question then. There was another question. What do you think are the most important factors affecting internet security in Taiwan? And could you give some examples?

00:08:08 TPU2

Factors affecting internet security in Taiwan... Well, there are two types of situations regarding firewall software. One is too expensive, and private companies may think that their data is not that important, so they won't purchase it. The other type is that they may not take information security seriously enough. Generally, they would hire an engineer or a related company to install it for them. And some of these companies may have installed it over a decade ago when there weren't as many frequent and numerous cyber attacks as there are now. So, back then, they just wanted something convenient to use and didn't upgrade it afterwards.

00:09:18 TPU2

Another type is that some companies only posted some basic information, but they didn't maintain it, so the information security firewall hasn't been updated. That's probably more or less how it is.

00:09:32 Interviewer

I see.

## Section C

00:09:34 Interviewer

Alright, let's move on to part C. This part is about discussing strategies for network attack defense. The first question is, based on your understanding, what is the overall network security plan of the Taiwan government? And what’s our opinions about these plans?

00:10:00 TPU2

Of course, this is a sensitive topic. In terms of this, there are some more sensitive issues to discuss.

00:10:14 Interviewer

It's okay, you can talk about whatever you feel comfortable sharing. If there's something you don't want to reveal, you don’t have to talk about it.

00:10:22 TPU2

I feel like we are still very serious about this, but actually...

00:10:26 Interviewer

Are you saying that the Taiwan government is very serious about it?

00:10:29 TPU2

Yes, about promoting network and information security, and software updates, they have been constantly working on it. However, hackers may sometimes be…, you know the red team? Have you heard of it?

00:10:50 Interviewer

Yes, the red team is more of the attacking part, right?

00:10:54 TPU2

Ah, yes, yes, exactly, just like playing basketball, one team is attacking, and the other is defending, whoever scores wins. The government department only focuses on defense, they won't attack. It's us the law enforcement officers who do the attacking job and will do the apprehension and investigation later on. So that's why I say this is a bigger issue, but compared to other countries in the world, we can't say that we are the top or the best, but our environment is unique, and our government has been consistently working on it.

00:11:42 Interviewer

Okay, got it.

00:11:45 TPU2

In fact, information security is taken quite seriously, and almost all public agencies, including private enterprises, are promoting it. As for the range and degree of their promotion, it should be said that overall, if there are better tools, then our firewall capabilities will be stronger.

00:12:09 Interviewer

I see.

00:12:10 TPU2

Right? It's a matter of level, in my personal opinion.

00:12:12 Interviewer

I see.

00:12:15 Interviewer

So you think they're all heading in the right direction, but there may be some resource constraints in certain areas?

00:12:30 TPU2

Resources...I don't know if this is a problem that needs to be addressed at a global level or if it's an individual problem. As individuals, we might feel that we have enough resources, right? But if we look at it from a global perspective and from the perspective of crime investigation, I think there is still much room for improvement. However, from the perspective of the public, they might feel that what we currently have is sufficient, so why bother improving? Yes, that's right.

00:12:58 Interviewer

Hmm, okay.

00:13:04 Interviewer

So let's move on to the second question. I think the second and third questions can be answered together. What do you think are the strategies for preventing online threats currently? And do you think these strategies are good or not? Is there any part that you think can be improved or done better?

00:13:28 TPU2

Of course, the stronger the software, the better it is, but stronger software is also more expensive. Hmm, it just requires more budget and funding.

00:13:38 Interviewer

Increase the budget?

00:13:43 TPU2

Yes, but sometimes there's only that much money, and they don't... it's also... right.

00:13:50 Interviewer

OK, so it's in terms of software?

00:13:54 TPU2

Yes, and of course, there needs to be regular promotion.

00:14:01 TPU2

For the first question, the promotional strategies have been regularly done, but as for the personal crisis awareness….hmmm.

00:14:10 Interviewer

Hmm, you mean that there is a lack of personal crisis awareness among the general public?

00:14:14 TPU2

Yes, because they haven't been victimized yet, they also think that it's unlikely to happen to them.

00:14:23 Interviewer

Right, right.

00:14:24 TPU2

Isn't that right? But on the internet, we do see a lot, and it seems like it's weak.

00:14:37 Interviewer

So currently, your prevention strategies are mainly focused on using software for prevention, but you also feel that these software tools need upgrading or improvement, is that correct?

00:14:58 TPU2

Yes, but the problem is, for example, if you surround a wall, and inside you have 100 sheep, but one of the sheep is very capable, it can jump over the fence, while the other 90-something sheep don't have the ability to jump over the fence. So, how do you prevent that one sheep from jumping out?

00:15:27 Interviewer:

Isolate it?

00:15:29 TPU2

Hahaha, that's my personal idea, but the problem is it's not possible. You have to uphold concepts like equality, freedom, and human rights, you can't isolate that one sheep. Some people might think, "Oh, I'll just raise the fence higher." But raising the fence higher means you need to increase your software and equipment, and so on, right?

00:15:57 TPU2

Ah, for the promotion, there are many promotions for it, all of them are promoting it. But the other 90-something sheep are already well-behaved, they won't jump out.

00:16:05 TPU2

But among them, there are one or two sheep who are hackers, who will try every means to break into the system. We can't say they have criminal factors in their minds, according to criminology, but they seek for excitement and establish their own power, their own achievements as hackers.

00:16:32 Interviewer:

Just to prove how capable they are, right?

00:16:35 TPU2

Yes, to prove they are very capable. So, this doesn't mean that we necessarily have to do something in a certain way. For example, in Southeast Asia, our defense is quite strong compared to neighboring countries, but we still get hacked, just like this theory.

00:17:06 Interviewer

Okay, now let's move on to the fourth question, and questions four and five can be answered together. Since we talked about prevention earlier, what are some strategies for dealing with a network attack that is happening currently?

00:17:24 TPU2

Of course, if an attack is currently happening, you need to find ways to prevent and control it. In addition to tracking the source of the attack, you need to strengthen your defenses as a stop-loss point to prevent further attacks and reduce damage, so you should take actions quickly.

00:17:50 Interviewer

So, in your opinion, what are some strategies that need improvement, or how can things be done better? Or do you think the current direction is sufficient?

00:18:07 TPU2

What can we do? Like I said earlier, if we don't care about human rights, we can just catch the perpetrator, but in Taiwan, we can't do that. We have to wait for the sheep to jump out of the fence and then we can catch it.

00:18:22 Interviewer

Oh, so we have to wait for the crime to happen and then take actions?

00:18:26 TPU2

Yes, because there is no way to defend against it before it happens. This is relativity. However, once it happens and you have to defend against it, but you might think that it’s a bit too late. So what can we do?

00:18:52 Interviewer

It's difficult, not just in Taiwan, but in other countries as well.

00:18:53 TPU2

Yes, that's right.

00:18:55 TPU2

Almost all the attacks we encounter are like this.

00:19:01 Interviewer:

Okay, so next we move on to the sixth and seventh questions. Just now we talked about the attack, and now that the attack has ended, you all must have some review measures. So, what do you think about the current review measures and steps you have taken? Do you think any changes are needed?

00:19:22 TPU2

Usually, we will make suggestions to them, but for the boss personally, they will go for better companies, such as defense companies or antivirus companies, to help them with the testing. After testing, they will upgrade their systems. To be honest, we usually make suggestions to them in this regard. And they will also do it themselves. But it’s easier for individual victims. Once the perpetrator is caught, there won't be any recurrence.

00:20:06 Interviewer:

Okay, I see.

00:20:07 TPU2

He wouldn't do it again, and he wouldn't attack him again unless he has an irreconcilable hatred towards the victim.

00:20:19 Interviewer:

OK, so the review measures are still considered acceptable, right? Understood.

00:20:25 TPU2

In fact, both the public and private sectors are similar. After the incident, they will all do a comprehensive upgrade and testing, find vulnerabilities, and patch them up.

00:20:36 Interviewer:

Okay, so mainly focus on the comprehensive upgrade, testing and finding vulnerabilities?

00:20:44 TPU2

Yes, find the vulnerabilities, conduct testing, and upgrade.

00:20:51 Interviewer

Ok。

00:20:54 Interviewer

So now let's move on to the eighth question. The eighth question is about what you just mentioned, which is your opinion on the public's general understanding of internet security. Do you think their understanding is sufficient?

00:21:09 TPU2

Well, we can divide it into the young, middle-aged, and elderly. The younger generation is more knowledgeable about the internet, so their general understanding of internet security is better.

00:21:27 Interviewer

So it's relatively sufficient, right?

00:21:27 TPU2

Yes, somewhat sufficient, because they often play on the internet and such, so they understand it to a certain extent. However, for the older generation, their understanding is lower. For example, grandparents may not understand it even if you explain it to them, right?

00:21:48 Interviewer

Okay, then we can move on to the ninth question. Because we just talked about how some age groups may have insufficient knowledge of the internet, does the government have any plans to improve education on internet safety for the public? Do you think these plans are good enough to improve the public's understanding of internet security?

00:22:32 TPU2

Of course, if they have exposure to computer-related courses and internet security education, then naturally, it would cover promoting awareness. However, when you promote awareness to them, their understanding is limited to simply using a computer. Whether it's targeted towards hackers or even just sending an email telling them not to click on that, the promotion is already aimed at raising their awareness, right? So if we promote the awareness and say, "Hey, don't click that one," do you think they will listen to us and follow what we tell him?

00:23:28 Interviewer

Yes, it's uncertain.

00:23:30 TPU2

Right, because sometimes they just can't distinguish it. But for us, we can tell whether a LINE (a messaging and calling app popular in eastern Asia) message or email is suspicious. The government also conducts checks, right?

00:23:44 Interviewer

Right, got it.

00:23:49 TPU2

Generally speaking, I still think that older people may be more vulnerable... if they use computers, they may be more likely to be attacked, but on the other hand, you said that there is education and promotion being done, right? But, the promotion can not only target the older generation and excludes the younger generation. It's universal and applicable to everyone.

00:24:16 Interviewer

In that case, how do you think we can improve? For example, the cybersecurity knowledge of those who are older?

00:24:26 TPU2

We still need to educate them, maybe we need to use examples.

00:24:33 Interviewer

Examples?

00:24:34 TPU2

Yes, special ones.

00:24:35 TPU2

Like the example we just talked about, the logic of a group of sheep, they may understand it better, but the problem is understanding is one thing, and implementing it is another. You may leave your phone number for them to contact you if they have any questions.

00:24:56 TPU2

Right?

00:24:57 Interviewer

Yeah.

00:24:59 Interviewer

Oh, and because the government is actually promoting it, for example, on the internet.

00:25:06 TPU2

Yes, you see, we almost see it as soon as we go to the websites, right?

00:25:08 Interviewer

However,…yes we can all see them.

00:25:10 TPU2

Including schools, you see, when you go to the websites, they will tell us about the security issues, what to pay attention to, what not to click on emails from unknown sources, and so on.

00:25:19 Interviewer

Yeah.

00:25:22 Interviewer

But in this way, older people may not see it? Because they may not necessarily search for the government's website.

00:25:30 TPU2

Yeah, that's right, they won't bother to do that.

00:25:32 Interviewer

Yeah, it's like it's really difficult.

00:25:36 TPU2

Oh.

00:25:38 TPU2

It's okay, this is something you can study in the future.

00:25:41 Interviewer

Maybe we need to promote it through channels that they are more likely to encounter.

00:25:47 Interviewer

But then again, there are very few of them actually encountering channels.

00:25:51 Interviewer

No problem. So for the tenth question, what do you think about the government's current plan for cultivating cybersecurity talents within schools or outside of schools? What do you think about these plans?

00:26:09 Officer Ye

Generally, it would be information-related courses. If you have exposure to these courses, then you will have the opportunity to be cultivated. If you don't have any related experience, then it's less likely for you to be exposed to these courses.

00:26:25 Interviewer

I see.

00:26:26 Officer Ye

Because if someone is not related to a certain field, then they may not see the value in learning it. For example, if someone is studying baking, they may think that cybersecurity is not related to their field. However, if someone is involved in the computer or network industry, then these talents would be within the scope of cultivation and education.

00:26:52 Interviewer

I see. Because what I know is that the government may offer some private courses to attract talented individuals to sign up.

00:27:05 Interviewer

So what do you think about that?

00:27:05 Officer Ye

Yes, but these courses may only attract individuals who are already involved in the computer or network-related industries. It may not be possible to fully popularize these courses to everyone.

00:27:22 Interviewer

I see, that makes sense.

00:27:25 Interviewer

So this is a plan specifically targeted at these talents. Do you think that the government's current programs are enough to attract these talents? Or are they enough to cultivate cybersecurity talents? Sometimes the government may go to schools or institutions to promote and say, hey, we have courses available, and then they may see if anyone is interested in signing up. Do you think this way of doing things is sufficient, or do you think there are other methods that could be better?

00:28:12 TPU2

Other methods that could be better…. For example, let's say we look at a company and we go to investigate and understand the situation when they are being hacked by hackers. Unless it's a company that deals with antivirus software or related areas, the boss or person in charge of the company would know about it. Otherwise, many companies, even their bosses, are completely unaware of these issues. Only the IT department knows about them. The IT department of a company, including schools, is the one that has knowledge about these matters. If you look at professors and assistants in various departments, unless they are specifically from the field of network-related departments, you won't find them having a deep understanding of these matters.

00:29:16 Interviewer

Right, they don't.

00:29:19 TPU2

Therefore, I think it's really difficult for the government to fully cultivate cybersecurity talents in the future.

00:29:27 Interviewer

Do you think it's necessary?

00:29:32 TPU2

Personally, I think it's enough to train cybersecurity personnel to be stronger and improve their software. If it's fully comprehensive, it's impossible. There are some departments in a school that are unrelated to cybersecurity area, and they may feel that the school is infringing on them, right? Let’s not say being excluded, but in their perception, it's like, "This is the information department. You are responsible for it, and we just don't want to be attacked. We will cooperate with you." This is the angle they come from.

00:30:12 Interviewer

I see, got it.

00:30:14 Interviewer

Do you think that what you just said was that it's enough to train these talented people in the information department, and do you think that the current training is sufficient?

00:30:26 TPU2

I think further on-the-job training is necessary, because some people may have graduated a long time ago and have not pursued further education. Unless you keep updating yourself, because the technology is changing rapidly. To be honest, as I just said, some private companies may still be using software from 10 years ago.

00:30:43 Interviewer

Hmm, I see.

00:30:51 TPU2

We don’t have to say it's low-tech. But indeed, it's very easy to be hacked if they don't update their software. Sometimes their maintenance personnel may not have enough budget, or they may think that no one would attack them normally. But they only realize the importance of security after an attack.

00:31:13 Interviewer

The importance of it?

00:31:14 TPU2

Yes, many companies have been tagged by hackers. Some hackers may just visit and tag them without any intention of causing damage. You see, they've tagged so many companies. Hackers can be categorized into good and bad. The good ones can help test and show that your anti-virus software is not working, but from our perspective, computer crime is illegal intrusion, which is a criminal act. So, it needs to be improved. But for the company involved, they may think it's not that important to spend money on it since their website is not that important.

00:32:14 TPU2

Yes, if it's important to them, then they will report it.

00:32:18 Interviewer

I see.

00:32:18 TPU2

Yes.

00:32:20 Interviewer

So, it's all about individual perception? Each company or group thinks differently about the importance of security?

00:32:27 TPU2

Yes, because it's a very practical issue!

## Section D

00:32:31 Interviewer

Okay, so now we're talking about the collaboration between the public and private sectors in the context of D.

00:32:37 Interviewer

So the first question is, for example, in terms of cybersecurity, what do you think of the concept of collaboration between the public and private sectors? Do you think this will really contribute to the development of cybersecurity?

00:32:55 TPU2

Of course, to some extent. I always say that the real experts are among the civilian. The government needs to borrow strength from the private sector. Honestly, personally, I think so.

00:33:12 Interviewer

Hmm, do you also think this is the trend for the future?

00:33:14 TPU2

Yes, if there's going to be collaboration, it really needs to be collaboration, not just one-sided decision-making.

00:33:20 Interviewer

So for the second question, do you know if there are any experiences of public-private sector collaboration in Taiwan currently?

00:33:30 TPU2

Yes, there are. Actually, in many areas such as the internet, like streaming on the world wide web, the governments don't interact with each other directly. It's done through some associations and other organizations that interact with each other around the world to help out. It's not just Taiwan, almost all countries in the world are the same because of factors such as different governments and policies. So this is actually quite necessary.

00:34:08 Interviewer

So for public-private sector collaborations like what you just mentioned, going back to questions three and four, do you think the mechanism and approach for collaboration is good or can it be improved?

00:34:24 TPU2

In terms of approach, of course, if the government can come out officially, their power will be greater because the private sector has no coercive power. They can only assist, right? So assistance is not much, but they will also think that if the government comes in sometimes, there will be too many restrictions and they will restrict a lot of things that shouldn't be restricted, which will cause a lot of inconvenience. So it's a double-edged sword and quite difficult.

00:34:52 Interviewer

Well, when you mentioned the streaming just now, you said it's only for some associations? What are they and how do they operate?

00:35:04 TPU2

How do they operate? For example, between Taiwan and the UK, we do have some exchanges and assistance through the internet.

00:35:11 Interviewer

Is it cross-border cooperation?

00:35:11 TPU2

Yes, it's cross-border cooperation. But it's not official, it's civilian. Through civilians, for example, if we want to catch a hacker, there are many things that we don't have with the UK. If we want to go through judicial assistance, it might take half a year.

00:35:34 Interviewer

I see.

00:35:35 TPU2

Right? But through civilians, I might be able to find the information next week. As I just mentioned, the power of civilians and the power of the government, the government has power, but it has to go through some lengthy and complicated procedures, causing some major difficulties and problems.

00:35:58 Interviewer

So it sounds like there is still very little cooperation between public and private sectors, because in the situation you just mentioned, it's more like cross-border cooperation between private sectors.

00:36:12 TPU2

That's an issue between public sectors, while private sectors working with each other are okay because there are fewer problems and it's faster.

00:36:23 TPU2

That's between governments.

00:36:25 Interviewer

I see.

00:36:26 TPU2

You see, we need to investigate a case through mutual legal assistance with the UK. For example, if we find out that a hacker is in the UK, then what do we do?

00:36:35 Interviewer

Okay, maybe?

00:36:36 TPU2

It's a big deal, but the private sectors don't have the power to assist us in executing our investigation. They can help us find out where he is in the UK, but they don't have the authority to help us catch him.

00:36:47 Interviewer

Hmm, so we still need the public sector to get involved?

00:36:48 TPU2

Yes, this is a problem for all countries in the world in the future. So you can research this topic thoroughly. It's a very novel one.

00:36:59 Interviewer

Okay, so now let's move on to the fifth question. Because we were just talking about the situation in Taiwan, does your unit have any experience working with private sectors in the past?

00:37:17 TPU2

Yes, we do. We still rely on civilian power, as I just mentioned. The experts are among the civilians, just like in the case of tracking Bitcoin and Tether. The public sector has no power. To be honest, we all rely on the civilian sector.

00:37:39 Interviewer

Bitcoin?

00:37:40 TPU2

It's like this all over the world.

00:37:44 Interviewer

So you also have some cooperation with the private sector?

00:37:46 TPU2

Yes, we must. It's necessary.

00:37:47 Interviewer

So do you think that cooperating with them is currently helping you in your investigative work?

00:37:56 TPU2

Yes, of course it is helpful. Otherwise, we wouldn't work with them.

00:37:59 Interviewer

Yes, so what do you think are the areas where can be improved, or are there any shortcomings? Because we already know the advantages.

00:38:13 TPU2

The public sector is like an elephant, it is too big and needs a lot of space to turn around, and it moves slowly. In contrast, the private sector is like a cat, it can turn around immediately and is more efficient. And as you mentioned, the mechanism of cooperation is also important. You can use this analogy to understand it. You can explore more on your own, but that's the basic idea.

00:38:46 Interviewer

Okay, so overall, the collaboration between the public and private sectors is necessary and the direction is correct, but more development is needed, right?

00:39:06 TPU2

Yes, there is still no good platform for collaboration between the public sector and the public sector in any country in the world.

00:39:15 Interviewer

I mean internally in Taiwan, you public sector collaborates with some private companies, but it seems like there is no mature mechanism yet?

00:39:39 TPU2

It's hard to say. You need to consider which aspect you are talking about. If you send an official document to someone, they will cooperate with you, right? Yes.

00:39:47 Interviewer

Oh, they have the power, right.

00:39:54 TPU2

So you say it is mature? To be honest, the mechanism for reporting cases is not okay.

00:39:57 TPU2

Almost all cases are reported after the victim has been victimized. Some units believe that it is confidential and do not want to provide information. For example, why is the fraud group so rampant? Because once we start investigating, they say they want to protect people's property and privacy, right? Otherwise, if the bank can provide this information quickly, the flow of funds of the fraud group can be tracked and stopped immediately. And the money can be seized in time. But if we wait for the victim to report the case, the police to investigate, and then chase the money, the money may have already been washed away. Isn't that a strange problem? Is the bank a private or public sector? It has official shares and others, but basically, except for Bank of Taiwan, which is a government-owned bank, other banks are profit-making and private units with official shares. You can use this problem to write about the fraud group.

00:41:07 Interviewer

Hmm, okay.

00:41:10 TPU2

Right? This way, you can describe it more clearly, and then add some of our crime prevention ideas to make your article very beautiful and complete.

00:41:21 Interviewer

Okay, thank you.