# Transcript

## Section A

00:00:00 Interviewer

Okay, we are now going to conduct an interview with TPR5.

00:00:05 Interviewer

Okay, let's start with section A and the first question. Since you are working in a private network security provider, this question has been answered, right, right, right, good.

00:00:15 Interviewer

The second question is about the unit you are working at currently?

00:00:19 TPR5

Yes, I am currently the director of the research department.

00:00:22 TPR5

So our research department is responsible for the second-line handling of security incidents in the company. For the first line, we have a technical support team or analysts to deal with it.

00:00:34 TPR5

If the analyst discovers a more severe or suspicious attack, they will pass this information to our research department for in-depth study. And some statistical information, such as the number of cases that occur each year. These annual and monthly statistical reports will also be forwarded to our research department to summarize the attack trends for the whole year. So these two aspects are more relevant to today's discussion.

00:00:58 Interviewer

The third question is about how long you have been working here?

00:01:05 TPR5

I have been working here for about 4 years.

00:01:08 Interviewer

Four years? Okay, good.

00:01:13 Interviewer

Before this, did you work in other units or in a related industry?

00:01:18 TPR5

Before, I was mainly in a pure research unit. I was pursuing my PhD. So, I spent a lot of time in school, studying and doing research.

00:01:27 Interviewer

Okay, then for the fourth and fifth questions, you mentioned your duties and responsibilities earlier. Could you elaborate on them a bit more?

00:01:38 TPR5

Yes, our department is responsible for a wide range of areas. We try to understand emerging threats, such as threats to cloud computing, AI, and the risks associated with connected vehicles and self-driving cars. We conduct research on the attack and defense techniques related to these newer topics, which may eventually lead to the development of future products.

00:02:05 Interviewer

Okay, I understand.

00:02:07 Interviewer

So, now we move on to section E on the next page. Because I am studying criminology, I actually approach this topic from a sociological and social science perspective, so I don't understand some of the specific terms in cybersecurity.

00:02:29 Interviewer

So sometimes I may need to ask you to explain more.

## Section E

00:02:34 Interviewer

Let's move directly to the first question in Part E. I want to ask you, based on your understanding, what are the main types of network attacks faced by Taiwan currently? What are the methods used in these attacks? Can you provide some examples?

00:02:50 TPR5

OK.

00:02:50 TPR5

Let me share some information here.

00:02:57 TPR5

Yes, there are many forms of network attacks, and they are quite complex. Moreover, it is a bit vague when it comes to network attacks. Therefore, I will first introduce a framework that is widely used, called the cyber defense matrix. This matrix categorizes the attacks into five levels. For example, for users, the most important level may be the protection of personal data and privacy.

00:03:33 TPR5

Some of the threats are related to data, such as the leakage of enterprise privacy, sensitive documents, or source code. There can also be incidents of internal user information being compromised. These threats can occur at the data level. At the network level, there are Distributed Denial of Service (DDoS) attacks that can disrupt the operation of services. Additionally, threats can extend to the application and device levels as well.

00:04:01 TPR5

Application-level threats are more focused on attacking services. For example, someone might attack your LINE application to steal chat records or obtain contact information from your LINE account. At the device level, attacks may involve infiltrating individual computers, creating backdoors, or encrypting data. Ransomware attacks are one of the most common examples of such attacks. So, we can categorize these attacks into five levels based on the objects you want to protect.

00:04:32 TPR5

So, because cyber attacks can be quite abstract, I'd like to ask which area you are most interested in?

00:04:43 Interviewer

Well, it's not that I'm particularly interested, but I tend to take a more comprehensive view.

00:04:51 TPR5

OK. I also want to mention in advance that the matrix is divided into each grid, which is each product or manufacturer. Therefore, the type of attack seen by each manufacturer may be different.

00:05:07 TPR5

In our case, we tend to focus more on the device and application layers.

00:05:13 TPR5

That means we may not have as much information to answer questions outside of these two areas.

00:05:19 Interviewer

OK, no problem.

00:05:20 TPR5

We tend to focus more on these two areas.

00:05:21 Interviewer

OK, so you can answer based on your company's experience.

00:05:25 TPR5

Yes, our main focus will be….I think it will be more like answers to the question D and F. However, let me first explain that our scope primarily involves Taiwanese enterprise clients. It includes government agencies, financial institutions, semiconductor companies, and some IT service providers. These are the main types of clients we serve.

00:05:49 Interviewer

Okay, got it.

00:05:50 TPR5

So in this field, we often encounter APT attacks, which are aimed at stealing company secrets or personal data. Attackers may lurk in the environment for a long time. As for recent trends, there has been a rise in ransomware attacks. These attacks have been particularly prevalent from the second half of 2020 to 2021 and 2022. Many of our domestic clients have been affected by these attacks.

00:06:33 TPR5

Right. Do you have any understanding of ransomware?

00:06:36 Interviewer

Yes, I have a rough understanding.

00:06:40 TPR5

If there are any terms that I haven't explained, please feel free to ask. The third area we have recently observed is attacks on financial institutions, which have become more common. Most of these attacks are carried out for economic reasons.

00:07:02 Interviewer

Okay, got it.

00:07:04 Interviewer

I have a question. You mentioned that ransomware attacks were particularly prevalent from the second half of 2020 to 2021 and 2022. Why do you think they became more popular during this time?

00:07:19 TPR5

For example, ransomware has its own business model, wherein the attackers operate within an underground network. This underground network has been developing and becoming more mature over time.

00:07:33 TPR5

The more relevant reasons include that, um, at that time, criminal currencies like Bitcoin were already very mature. These platforms were very suitable for conducting criminal transactions. So now, ransomware will probably use this kind of platform to deliver ransom. Um, that's the way to do it.

00:07:53 TPR5

So probably starting in 2019 and 2020, maybe from 2018, 2019, 2020, criminal currencies became more complete. So it was easier for ransomware to use this platform to deliver ransom and avoid being traced. So it expanded to the emergence of ransomware. The second one is during this period, they have a relatively new software business model called "big game hunting." In the past, the older types of attacks may have targeted regular users or they would scatter ransomware like an advertising campaign, reaching anyone available.

00:08:46 TPR5

But then it turned more towards precise attacks, where they studied certain companies and industries to see who was making the most money and focused on attacking them. This way, the rewards they received were much higher than attacking individuals. After this business model appeared, ransomware became very popular during this period, because once people knew this trick, they began to set up various ransomware organizations to carry out these attacks.

00:09:18 Interviewer

Okay, thank you.

00:09:19 TPR5

On the APT side, on the other hand, APT has been around since…., possibly starting before I joined the company in 2014 or 2015. The main issue with ransomware is the political situation in Taiwan and China. So whether it's official attack groups or unofficial attack groups on the other side (China), Taiwan is a convenient or suitable target for attack.

00:09:53 Interviewer

Next, let's move on to the second question. As you mentioned earlier, I'd like to ask: What do you think are the main targets of cyberattacks in Taiwan currently? And what are the reasons for them being targeted?

00:10:11 TPR5

OK, this question can vary depending on the industry. If it's more government-related, it's usually related to political intelligence, such as political figures' schedules or internal meeting records. We see that there are more attacks on governments to steal information.

00:10:37 TPR5

For enterprises, as I mentioned earlier, it's ransomware, so encrypting data and ultimately making money through stealing or encrypting data is their goal. For financial institutions, their targets may be their financial flow systems, and they may want to steal information such as credit card information and then sell it outside.

00:11:07 TPR5

So it can vary depending on the industry.

00:11:09 Interviewer

OK, I understand.

00:11:11 Interviewer

Also, I want to ask, is there any particular industry that you think is more vulnerable to attacks? Is there a specific industry or several industries?

00:11:26 TPR5:

Currently, it seems that the government is still receiving more attacks. That's because as a whole, the government is more vulnerable. To clarify, when it comes to being attacked and being successfully attacked, we may be talking more about the latter. Today, I think we are seeing more successful attacks where the attackers have already infiltrated into corporate systems. These corporations may have defenses such as firewalls or antivirus software that detect thousands of attacks, but some of those attacks may be ineffective.

00:12:01 TPR5

What we observe is that the most significant impact and effective execution of cyberattacks occur in the later stages, where the attackers may have already infiltrated our environment and initiated operations. In this phase, we tend to see a higher number of attacks targeting government entities.

00:12:15 TPR5

The main reason is that the government's defenses are not as complete, and the quality of personnel is not as consistent. For example, some phishing emails are more likely to get through.

00:12:26 Interviewer:

Okay.

00:12:29 Interviewer:

So, it's the government that has less complete defenses?

00:12:35 TPR5:

Yes, and the quality of government personnel is lower. For attackers, phishing is still the easiest and fastest way. Financial institutions, on the other hand, should have a clearer understanding and better defenses to prevent these things from happening.

00:12:50 Interviewer:

Okay, got it.

00:12:54 Interviewer

So, let's move on to the third question. What do you think are the factors that affect Taiwan's internet security?

00:13:02 TPR5

Well, I think the most significant factor influencing Taiwan's cybersecurity is its relationship with China. This indeed has a considerable impact. During periods of heightened tension or significant events such as major holidays, Taiwan may face increased cyberattacks. For example, during presidential inaugurations or elections, as well as around National Day, such attacks tend to occur more frequently.

00:13:41 TPR5

Another point worth mentioning is that the semiconductor and manufacturing industries in Taiwan are gradually gaining international recognition for their strength and profitability. As this information becomes more widely known, these industries are also becoming targets of cyberattacks more frequently.

00:13:58 TPR5

Yes, so the popularity of the semiconductor and manufacturing industries will also affect whether they will be attacked.

00:14:06 Interviewer

Okay, great.

## Section F

00:14:09 Interviewer

So now let's move on to Part F. Alright, the first question in Part F is about the cybersecurity aspect. Could you please share what kind of technology and services your company provides to clients in this field?

00:14:23 TPR5

This goes back to this diagram. It might be easier to explain it this way.

00:14:29 TPR5

This chart represents the vertical axis as the targets to be protected, and the horizontal axis as the defense stages. For example, in the early stage, "identify" means identifying existing issues. For instance, if we find someone who falls for phishing attempts regularly, we must take them, train them, and then send them back so they won't be vulnerable to phishing attacks. This step involves identifying the problems we have.

00:14:55 TPR5

"Protect" refers to the stage where we take action to block the attacks when they occur. For example, using antivirus software or a firewall to block the attack as soon as it happens falls under this category.

00:15:10 TPR5

And "detect" means that the attack has already occurred, but we couldn't immediately block it. However, we have set up measures to detect and raise an alert, informing us that something has happened, and we need to act quickly to address the issue.

00:15:23 TPR5

And after the incident occurs, I need to respond, right. If my computer is compromised with a backdoor, I need to know how to handle it. There is a hacker using a specific domain IP to control my computer, so I may need to add it to the firewall to block it.

00:15:37 TPR5

And finally, recover. If we are attacked today and our data is stolen, how do we go about recovering? Yes, and if our machines are deleted, and the files inside are also deleted, how do we recover from that? These are the kinds of scenarios we need to consider for recovery.

00:15:47 Interviewer

Okay, got it.

00:15:48 TPR5

So the entire defense can be divided into these 25 grids, and we are better at the blue part that is marked out. Specifically, we are more proficient in the detect and response areas, from the network, application to the device level.

00:16:07 TPR5

n this part, we usually focus on providing more specific and effective solutions. For example, we install endpoint software or network-level programs on the client's computers to monitor various activities within the enterprise. We use techniques such as memory learning to identify traces of attackers. Once we detect such traces, we notify the blue team to initiate a response. Therefore, our main role is to handle the detection and response aspects of defense. We inform the client about suspicious behaviors that may indicate hacker activity and provide recommendations on how to deal with them. In the end, we summarize the malicious programs and provide information about the IP domains used by the attackers, which the client should then clean up. If there is any data leakage, we also help with recovery measures.

00:17:08 TPR5

So our scope is roughly in this area.

00:17:13 Interviewer

What does this mean? Is it SIEM? CTI?

00:17:18 TPR5

OK, it's SIEM. It's a log aggregation center. Our machines all have some logs, and security products also have logs or security alerts.

00:17:30 Interviewer

I see.

00:17:31 TPR5

Attacks usually don't happen with just one event. Let me show you another framework.

00:17:39 TPR5

You don't need to understand this framework, but it talks about how many techniques attackers might use. The framework shows the stages of an attack, so an attack isn't just one thing happening. It might be a series of behaviors. For example, attackers might first steal a user's account and password, which falls under the "initial access" part of the MITRE ATTACK framework.

00:18:05 TPR5

After breaking in, for example, if they are now within the HR’s computer. Then they might want to get into the general manager's computer, and they might first jump to, say, the R&D computer, which is called "lateral movement."

00:18:20 TPR5

Yes, on the R&D computers, they may collect some information, see if there is anything in there, if it is responsible for managing? Does it happen to manage the general manager's computer? What are the general manager's computer account and password? After obtaining that, they can get into the general manager 's computer, so the final step is to control it. We will call this command and control, to control the general manager's computer, and then after obtaining the data, they will leak the data externally, which is called exfiltration.

00:18:47 TPR5

Of course, some ransomware software will encrypt your computer, so the attack is a long series of events. Each event may occur on different machines or different software, and these may all have some logs.

00:19:02 TPR5

Actually, each cybersecurity product will generate alerts.

00:19:07 TPR5

So these alerts will have a very large number of logs. You can think of it like the police investigating a case, I have a lot of clues, these clues will be put on this SIEM platform. So there may be footprints at the scene, bloodstains, and weapons, and these things are aggregated into a middle database called SIEM. What we do more is EDR or NDR, based on the original log or based on SIEM information.

00:19:37 TPR5

And then we go inside to find out what the whole path of the attack is? If SIEM may be an observation, a single piece of information put together, then what we do is reassemble the single piece of information into a case.

00:19:50 TPR5

Yes, so we are like detectives, saying I see this bloodstain, I see this weapon, and then I infer how the person was killed, like that.

00:20:02 Interviewer

What are EDR and NDR?

00:20:05 TPR5

So this DR is detector and response, so actually in this framework it directly corresponds. I think its goal is like what I just said, I found the attacker's clues from so many logs, and then pieced them together into a story, and then I have to tell the unit's person in charge how to respond.

00:20:24 TPR5

And E and D, they just monitor different ranges. EDR is on the endpoint, doing analysis on the computer, while NDR is at the network level.

00:20:37 Interviewer

OK.

00:20:39 TPR5

Another thing we are working on is the CTI (Cyber Threat Intelligence) part. It's basically the part about threat intelligence. If we take an example of crime, there might be international criminal organizations that share information about criminals or criminal methods with each other.

00:20:57 TPR5

CTI is doing this in the information security field.

00:21:01 TPR5

We collect some threat intelligence provided by other vendors, know what kind of attacks are popular recently, and ask our customers to take preventive measures. Of course, we also provide some threat intelligence to share with the community. So these few parts are what we do more of in terms of service scope.

00:21:39 Interviewer

Since you just talked about for the second question earlier.

00:21:42 TPR5

Yes.

00:21:43 Interviewer

Let’s move on to the third question.

00:21:48 Interviewer

The third question is about the main reasons why these customers seek your services.

00:21:53 TPR5

Well, there are mainly two factors. The first one is that they are hacked, so they come to us for help.

00:22:02 TPR5

This is common. They may not have thought about improving their own cybersecurity capabilities beforehand. They typically only seek our help after experiencing cybersecurity issues and needing assistance to address them. The second major source is regulatory requirements. For example, financial and government units need to comply with regulations, so they will be more active in implementing certain defense mechanisms if the regulations require them to do so.

00:22:34 Interviewer

So they usually only come to you after something has happened, and they don't usually plan ahead?

00:22:40 TPR5

Yes, in fact, there is not much pre-planning involved. Usually, clients approach us after an incident has occurred. So, we often joke that the "black industry" (referring to attackers) is the one driving advancements in the cybersecurity industry.

00:22:56 Interviewer

Okay, let's move on to the fourth question. The fourth question is about what aspect of cybersecurity most of your clients are lacking in.

00:23:09 TPR5

Alright, on this matter, I think first of all, from a general perspective, as we introduced this framework, you can see that ensuring cybersecurity is not a single task.

00:23:23 TPR5

Yes, we only cover this one aspect.

00:23:27 TPR5

There are many different products or defense aspects that need to be addressed.

00:23:31 TPR5

So first of all, I think most clients don't have this concept, and they may expect a total solution. Therefore, they haven't really thought about the overall defense architecture. Moving on to what most clients are doing, they are generally more proficient in the protection layer, but the parts beyond protection are not yet mature. In Taiwan, in the past year or two, some regulations have been put in place for the financial and government industries, which require the implementation of detection and response mechanisms.

00:24:19 TPR5

So, starting from 2022, these mechanisms are gradually maturing, but compared to the protection layer, they are not yet as mature. Protection tools such as anti-virus software, WAF, or firewalls have already been implemented in most enterprises or government units, so this layer is usually more mature. The focus is now on the subsequent layers.

00:24:42 TPR5

Yes, and these layers are slowly maturing. So I think the next area that everyone will focus on is the Respond layer.

00:24:51 Interviewer

Okay, for the fifth question, I want to ask what are the main forms of network attacks that you often deal with?

00:25:07 TPR5

Yes, in our field, we often encounter attacks on devices, applications, and networks. The main types are APT attacks, ransomware, and backdoor attacks, and other types of malware.

00:25:24 Interviewer

I see.

00:25:25 TPR5

How to deploy? The post-intrusion behavior of attackers, such as when they have already entered your computer and planted backdoors, is what we commonly observe and handle in our scope.

00:25:45 Interviewer

Okay, then for the next few questions, they may not be phrased very well, but if you can answer them, just answer the part you can answer.

00:25:57 Interviewer

So, um, for the sixth question, I want to ask, I think the sixth and seventh questions are quite similar to what your company is doing. I want to ask because for the sixth question, I want to ask, just now you mentioned that attackers…people usually do quite well in the front-end defense, and many antivirus software programs also do quite well.

00:26:22 Interviewer

However, when attackers really break through this line of defense, they enter the back-end, so it may be related to cyber resilience, and what mechanisms do you have for reducing damage and event management?

00:26:41 Interviewer

But you just answered it a little bit, like detect and response.

00:26:46 TPR5

Because what we are doing is more like, if the attacker has already broken through the front-end defense, how do we assist the client in understanding the situation and help them with the subsequent actions to reduce the damage? Here, we will first do a rough count of the scope of the impact of the case, which computers have been affected, which permissions he can retrieve, which users have already been controlled, and which data has already been leaked.

00:27:18 Interviewer

Okay, got it.

00:27:20 TPR5

Then probably these three levels, and then, in this part, it requires a lot of discussion with the other party's blue team because everyone's situation is different, and then discuss the extent of the damage, how should we recover and manage it, for example, with users, I might be able to change passwords, but if data leaks, then it might not be possible, and I have to report upwards that the data has leaked, and then evaluate the impact on the business or take some preventive measures in advance, and as for the machines, for example, machines commonly used, we often encounter a situation where we need to reduce the damage, for example, for some critical servers, they may not be shut down or even accessed because nobody knows what might happen, so in this situation, we cannot ask the customer to reinstall the computer and actually delete the malicious files. We might suggest protecting and isolating the machine, place it in the internal network, and don't allow it to connect to other computers, and then reduce the scope of this damage.

00:28:30 TPR5

What about network resilience? For this, I am curious about your definition.

00:28:37 Interviewer

Actually, it's what I mentioned earlier. Because I designed this question in English first, and then translated it into Chinese. So, what I wanted to ask is about cyber resilience. I just wanted to ask because, from my understanding, and I may not be very precise, but I think this way is more accurate, the concept of network resilience is somewhat like…..For example, in a company, if we need electricity to operate but suddenly there is a power outage, is there any backup power that can allow the company to continue operating and not be completely shut down? It's a similar concept for networks.

00:29:27 TPR5

It seems like our definitions are similar. I just divided it into how to differentiate it more.

00:29:39 Interviewer

Into how many layers?

00:29:39 TPR5

Several layers, maybe, first is to avoid being attacked, right? Then the second is when attacked, you won't be directly knocked down and die.

00:29:52 TPR5

Yes, even if you encounter a network attack, you can still have a certain degree of business continuity, and quickly restore your business operations afterwards.

00:30:05 TPR5

Let me see what I wrote before, I have forgotten, okay, let's first look at these two parts, the "withstand" and "recover" parts. What we do more here is, well, it also echoes what I said earlier that an attack may be a series of actions.

00:30:24 TPR5

For example, the final step of an attack is to encrypt the entire company's computers. The attacker may need to invade your domain control server, which can control all computers, before encrypting all files on the machines. So if you can detect the attacker's traces early and block him or make his attack more difficult, then the later part won't happen, and I can meet this part, which is more about anticipating and withstanding. If we are attacked today, probably only a few computers are affected, and if he hasn't touched the most important domain server, then I may not experience a situation where the entire company is encrypted, and only part of the computers are encrypted.

00:31:10 TPR5

So what we do is to monitor these vulnerabilities and alerts early, and notify customers to take appropriate action when we detect these suspicious activities, and strengthen our ability to withstand such attacks. In the recovery part, as I mentioned just now, I will check the scope of the damage and suggest to the customer how to recover.

00:31:35 TPR5

So, our focus is more on these two areas, and of course, after the incident, the customer may use our data to review and analyze what happened, what were the issues, and how they can improve in the future, which falls under the "Adapt" part.

00:31:49 Interviewer

So, for the seventh question, I want to ask if you think the cyber resilience mechanism that your company provides in this area is good or not? Or where do you think it can be improved?

00:32:07 TPR5

Of course it’s good.

00:32:12 Interviewer

OK.

00:32:14 TPR5

I think it's good for companies to have this kind of service because it helps with the overall health of their business operations and, as I mentioned earlier, with cyber resilience. The part that we may be lacking or, to put it another way, the part that we may not be focusing on is the anticipatory part. We focus more on the detect and response aspects.

00:32:41 TPR5

Right, so from our perspective, we mainly cover the "Detect" and "Response" parts within these nine areas. As for the rest of the CDM (Cybersecurity Defense Matrix) scope, especially in terms of "Data" and "User" detection and response, we haven't been heavily involved in those areas. In such cases, we might recommend the client to evaluate and consider other products to complement and fill in those gaps. Because there isn't one comprehensive solution that covers everything, we focus on guarding this area, while other aspects may require the involvement of other vendors or technologies.

00:33:17 TPR5

Yes, so for data and user as well as recover, these two areas are important for resilience, but we don't cover them as much, especially in the last part, recover. This part is more complicated because it will be related to the customer's operational situation, and it is difficult to automate and solve the customer's problems on a large scale.

00:33:40 Interviewer

OK, so for the eighth and ninth questions, I think they can be answered together. I want to ask, does your company feel that there are any areas where your technology services are lacking? I don't mean to criticize, but because you are providing these services, there must be some aspect that you think can be improved or developed more completely. Are there such areas?

00:34:09 TPR5

Um, first of all, the biggest difficulty we encounter is communication and coordination with clients. This part is actually quite challenging because, as mentioned earlier, each client's situation is different, and it is difficult for us to tailor a set of methods specifically for each client. They also have their own difficulties, such as some machines not being able to install our system, or not being able to provide us with certain data. So, sometimes when we are doing detect and response, our visibility and the range we can see are relatively small. These are some areas that I think still need improvement.

00:34:59 Interviewer

So, how do you think you can improve in this aspect? Do you call the clients over and educate them?

00:35:08 TPR5

Well, education and training is certainly one method we have tried. For example, if the overall cybersecurity level of blue teams and cybersecurity concept in Taiwan are improved, then they will better understand why we need to do these things.

00:35:25 TPR5

It will make it smoother for us to cooperate with them.

00:35:32 TPR5

It doesn’t have to be training. Promoting cybersecurity concepts through some public platforms, such as the Taiwan Hacker Association, which holds conferences that many people attend, can help spread more accurate cybersecurity knowledge. This way, clients can also understand why we need certain data and why we need to install certain programs, and they can also understand that in order to avoid risks, they may need to sacrifice some performance issues.

00:36:03 Interviewer

OK.

00:36:05 Interviewer

The tenth question is about whether your company has any plans for future expansion and development in terms of technology and the services you provide?

00:36:18 TPR5

Okay, let me think about how to answer this. Well, first of all, our team is a research-oriented one, and we are continuously developing new things. So, in terms of new areas, we focus on conducting research and developing prototype products. Currently, our primary focus is on Active Directory (AD) related activities, such as permission analysis and attack prediction. AD is a system used by many enterprises, it's a Microsoft system mainly used to manage Windows computers and their data, and most companies adopt this management mechanism.

00:37:07 TPR5

On AD, it records information about users, as well as the permissions settings that determine which computers and objects a user can access.

00:37:17 TPR5

In our past observations, attackers can easily move laterally and go undetected, at the LM level, due to poorly managed AD permissions.

00:37:26 TPR5

Or there may be some vulnerabilities in our AD, so I think this is a big problem.

00:37:30 TPR5

So, in our recent efforts, we have started developing such products. We aim to analyze all the account permissions on AD, the relationships between account permissions and objects, and identify potential attack paths that attackers might use. By doing so, we can proactively patch or improve these vulnerabilities. In essence, it's about analyzing and simplifying the internal account permissions and access control within enterprises. For example, if we find a misconfiguration where a temporary worker has access to the entire company's data, we can address and rectify it early on.

00:38:11 TPR5

Another issue is related to the Internet of Vehicles (IoV). This is slightly different from today's topic, but we have also invested some people in researching IoV to explore possible attacks and defenses in the future.

00:38:23 Interviewer

You mean IoV?

00:38:23 TPR5

The Internet of Vehicles (IoV) is EB, which refers to smart cars and autonomous vehicles.

00:38:29 Interviewer

Autonomous vehicles?

00:38:30 TPR5

Yes, autonomous vehicles and similar vehicles.

00:38:35 TPR5

Finally, we will also move towards the direction of measurable risk.

00:38:42 TPR5

For example, the puzzle is slowly coming together, but the problem we face is that the security team needs to report to their bosses on how much the overall risk has decreased. What is my performance for the year ? These all need us to quantify the risks.

00:38:59 TPR5

So, based on these products, we aim to establish a quantifiable risk assessment index that provides enterprises with clear indicators of their internal and external risks. This will allow them to understand how much they have reduced risks by implementing these measures during the year. Therefore, we are focusing on improving and strengthening the measurement of both internal and external risks in the future.

## Section G

00:39:20 Interviewer

OK, then let's move on to the part G. The first question I want to ask is about your opinion.

00:39:26 Interviewer

In your opinion, do you think that cooperation between public institutions and private sectors like yours is helpful for the development of cybersecurity on the internet?

00:39:36 TPR5

Yes, I think so.

00:39:37 TPR5

It definitely helps the development of cybersecurity. Firstly, because a large part of what we deal with are cybersecurity incidents that occur within the government, we must have some cooperation with public institutions. So if we have cooperation with public institutions, the first thing is that the collaboration process will be smoother. As for education and training, or promoting correct cybersecurity concepts, I think this is something that public institutions must do.

00:39:58 TPR5

So, in fact, the United States has done quite well in this regard. They have a Cybersecurity and Infrastructure Security Agency (CISA) responsible for declaring cybersecurity policies and information.

00:40:07 TPR5

This is very good, so we also hope to work more closely with government departments to promote correct cybersecurity concepts.

00:40:15 Interviewer

OK, the second question is, as far as you know, is there any mechanism or model for cooperation between public and private sectors in Taiwan's overall cybersecurity?

00:40:25 TPR5

Here, we do have some cooperation, such as intelligence sharing with some Taiwanese government agencies responsible for cybersecurity.

00:40:38 Interviewer

Are you talking about your company?

00:40:39 TPR5

Yes, we collaborate with some government departments on intelligence sharing. When we identify new attack techniques or vulnerabilities that may have an impact, we provide timely notifications. Additionally, we partner with educational institutions and departments to train and cultivate future researchers and cybersecurity professionals. Moreover, there are other collaborations, but I apologize for not being able to disclose further details to maintain confidentiality.

00:41:03 TPR5

We even engage in de-identified data sharing, ensuring that secure information can be collaborated with certain academic research units.

00:41:16 Interviewer

Okay, then let's move on to the third question. What do you think of the current cooperation model? Do you think it is effective?

00:41:19 TPR5

Well, I think the results are not that satisfactory because there is a lack of comprehensive national-level strategies and processes. The efforts at lower levels seem more like patching up what's missing, creating a sense of incompleteness. So, there isn't a big overall...

00:41:39 Interviewer

A concept of patching up one wall while another wall springs a leak?

00:41:39 TPR5

Yes, yes, yes, that's the issue. They come to ask for help when problems arise, but there isn't an overall framework explaining why this action is necessary.

00:41:47 Interviewer

That means there is still no systematic or...

00:41:49 TPR5

Yes, there is no systematic national security level and no systematic cybersecurity strategy.

00:41:55 Interviewer

In that case, let's move on to the next page.

00:41:59 Interviewer

Yes, for the fourth question, you feel that improvement can be achieved by having some national-level strategies for cybersecurity. This means the government should release comprehensive cybersecurity policies to raise awareness and understanding among the general public and organizations.

00:42:16 TPR5

Yes, I think if it's a more common collaboration model, it's usually not very systematic. It's more like if I need something, I might set up a project and do something, but there's not a lot of overall planning. So sometimes things like resources aren't reused. For example, Unit A and Unit B might both be doing the same thing because they see the problem and take similar actions. However, this could result in some resource wastage. Or, they may feel that they lack a specific project, but that project might have some prerequisites, and without those prerequisites, it may not be very effective.

00:42:51 TPR5

And without anyone planning to achieve these initial steps, the effectiveness of the subsequent actions won't be as high.

00:42:55 TPR5

So we might need a more systematic approach, where we have different plans to execute in order to achieve our goals. These plans are interconnected, where the effectiveness of the first plan becomes input for the second plan. Therefore, a comprehensive government-led cybersecurity framework and strategy are required.

00:43:18 Interviewer

Okay, for the fifth question, you mentioned earlier, l your unit collaborating with the public sector, do you have any experience to share or what is your collaboration model like?

00:43:36 TPR5

Right, so for this part, there are three aspects. The first two parts have been mentioned before, like sharing intelligence with the government's cyber security department and collaborating with the education department to cultivate talent. The third part is more scattered, and may not be considered as public-private sector collaboration. In Taiwan, most situations involve various departments or units coming to us and using our services and products.

00:44:07 TPR5

So, the third part will result in everyone actually encountering the same problems, but each one is different.

00:44:14 Interviewer

It doesn't necessarily have to be a public institution, it could also be an enterprise or the government?

00:44:18 TPR5

Yes, it should be government departments, but maybe 10 government departments come to us separately, and then go to use our products and, um, use our services. This will cause some inconsistencies because they each come to us separately, and each solution they use may be different. So, the strength of security may be different. These can actually be reduced to some extent because everyone has done the same thing many times.

00:44:52 TPR5

So, this may be the various departments under each department, their policies are different, and there is no integrated way to cooperate with us.

00:45:06 TPR5

In the previous part, um...

00:45:14 TPR5

The collaboration with government departments is often challenging for us as it is difficult to measure certain indicators. When we share intelligence or information with the government, we often lack visibility into the effectiveness of that information. We don't know how many people have accessed the shared data, nor do we have a clear understanding of the scope of impact that the reports or intelligence have had. This leads to difficulties in assessing the effectiveness of our collaboration when evaluating internal performance KPIs.

00:45:56 Interviewer

OK, in that case, we can respond to question six and question seven because you just mentioned that this kind of collaboration can be improved in certain areas. Can you elaborate on that?

00:46:10 TPR5

Let me think if there is something else in Taiwan.

00:46:12 Interviewer

Actually, you already talked about it earlier.

00:46:15 TPR5

Actually, there is one more thing. The difficult part of cooperation is the government department's requirement for certain documents. For example, in Taiwan, the document requirements are more stringent.

00:46:29 Interviewer

So, it’s cumbersome?

00:46:34 TPR5

Yes, dealing with complex documents and processes can be very labor-intensive. So, this aspect is something we believe should be improved, as the government often struggles to keep up with the faster execution pace of private enterprises.

00:46:49 Interviewer

OK, so in terms of document procedures, some improvements should be made to make it easier.

00:46:55 TPR5

Yes, for many collaborations, we feel that while I can use the manpower of one researcher to complete this collaboration project, they may need to use four manpower, and the other three may have to deal with document issues.

00:47:13 Interviewer

OK, I understand.

00:47:16 Interviewer

Well, I think that's about it. Thank you.