# Transcript

## Section A

00:00:01 Interviewer

We are now doing the interview with TPR1.

00:00:06 Interviewer

Okay, let's start with Section A. The first question is relatively simple: Are you currently working for a private network security provider? Can you tell me what unit you are working at?

00:00:22 TPR1

I have been working at [a private company] for almost eight years now.

00:00:27 Interviewer

OK.

00:00:27 TPR1

I am currently the head of the Information Security Office. Because the Taiwan Stock Exchange requires companies to be listed in three different levels, our company belongs to the B level. Therefore, before the end of next year, an independent unit with a dedicated supervisor must be established. I am the head of this unit. In my eight years at [a private company], my responsibilities have included ISO 27001, information security management, policy deployment, technical resources, advanced technical support, and strategic planning.

00:01:13 Interviewer

Okay.

00:01:15 Interviewer

Alright, that's pretty clear.

## Section E

00:01:18 Interviewer

Next, we'll move on to the E section, because the previous one was about the police unit.

00:01:25 Interviewer

Okay, so if we move on to section E, for the first question, I want to ask, in your understanding, what is the most common network attack that Taiwan is facing now? And what are the modus operandi? You can also give some examples.

00:01:40 TPR1

I think in recent years, the main attack that Taiwan has been facing is the WannaCry ransomware attack. Since WannaCry, there have been many variants, including BitLocker 2.0.

00:01:52 TPR1

They even operate like suppliers, welcoming insiders from companies to join them as partners. If successful, meaning if the company pays, they will get a commission. So WannaCry is the main attack that Taiwan is facing now, and the main modus operandi is usually through social engineering.

00:02:15 Interviewer

Social engineering.

00:02:16 TPR1

Social engineering, starting from stealing your credentials, and then usually intruding from the domain controller (DC), and then using the domain controller to deploy the attack globally, so that the encryption can be handled in one go.

00:02:39 Interviewer

Okay.

00:02:42 Interviewer

Actually, WannaCry started around 2016 to 2017, right? At that time, the attack also affected the whole world, including the UK.

00:02:51 TPR1

Many, because it's a vulnerability in the SMB 1.0 file sharing, so if you have file sharing open or haven't patched the vulnerability, yes, there's a specific term for it, "Blue Tears" or something like that in Interviewernese. If the vulnerability hasn't been patched, it's actually very simple to be attacked, and because the way it spreads is very simple, using tools, you can quickly create an encrypting virus. But because it's so simple, most basic antivirus software, which relies on patterns, similar to COVID-19, needs a pattern to be identified first before it can find a solution for it. However, because this attack is so simple and fast, typical network defenses can't block it effectively.

00:03:39 Interviewer

I see. Yes, at that time, it affected the UK's healthcare system, right?

00:03:44 TPR1

Yes, hospitals, too.

00:03:46 Interviewer

Yes, Taiwan too. Alright, let's move on to the second question. So, the second question is, because we just talked about the methods of attack, what do you think is the main target of cyber attacks in Taiwan now? And what do you think is the reason for it?

00:04:04 TPR1

You mean internal?

00:04:06 Interviewer

Both are okay.

00:04:07 TPR1

Oh, actually, I think the main target of the attack is still the same. Internally, it's the core, as I mentioned earlier, the domain controller, also known as DC. The domain controller can deploy policies through computers that join the domain, allowing for large-scale, global, simultaneous attacks.

00:04:15 Interviewer

Mm-hmm.

00:04:25 TPR1

And, furthermore, your external services are quite vulnerable. Nowadays, attackers will certainly try to find a way to breach from the outside, for example, through your official website or any third-party services you have on the internet.

00:04:41 Interviewer

Besides that, what do you think is the main target of attack, for example, which industry is more vulnerable to attacks?

00:04:51 TPR1

The manufacturing industry.

00:04:53 TPR1

Taiwan started as a manufacturing-oriented country, so many small and medium-sized manufacturing industries have grown into large-scale operations. For instance, we specialize in industrial computers and focus on the sampling aspect.

00:04:55 Interviewer

Okay, got it.

00:05:03 TPR1

In fact, for Taiwan's manufacturing companies, whether they are listed or not, they generally prioritize investing in research and development, particularly in industrial R&D. Therefore, their focus on cybersecurity investment is relatively lower. This applies to the manufacturing industry. Of course, the government is also a major target for cyberattacks; that's for sure.

00:05:26 Interviewer

Okay, let's move on to the third question. What do you think are the factors that affect Taiwan's cybersecurity overall? Can you give some examples?

00:05:40 TPR1

I feel that the biggest weakness in Taiwan's cybersecurity lies in people, particularly the end users. They lack awareness and knowledge about cybersecurity, whether it's in a company or private domain. Therefore, I believe it is the responsibility of companies to address this issue through ESG and CSR initiatives. Companies should provide their employees with cybersecurity information and know-how during their time with the company so that they can apply it in their personal lives. Ultimately, the security factor depends on people and how much companies are willing to invest in cybersecurity. For example, employees in certain industries like the service or food industry may not have access to such information. In such cases, it's crucial for the government to step in with awareness campaigns or initiatives, such as the Ministry of Digital Affairs.

00:06:43 TPR1

In the future, the Ministry of Digital Affairs may develop an online platform or a virtual school to provide the public with knowledge about cybersecurity, so that the overall cybersecurity of the country can be improved.

00:06:47 Interviewer

Okay, so you think that the problem mainly lies with people who lack knowledge and common sense about cybersecurity, making them vulnerable to cyber attacks?

00:07:13 TPR1

Yes.

## Section F

00:07:15 Interviewer

Alright, now let's move on to the section on F and talk about strategies for defending against network attacks. I wanted to ask, in terms of network security, your company provides what kind of technology and services to customers?

00:07:32 TPR1

Actually, we are not a security provider. We are not a cybersecurity company that provides security products or anything like that. For manufacturing industries, the service we provide to customers is to make sure that their customer data or confidential data will not be leaked. Customers wouldn't want to see their product's entire engineering drawing or some related confidential files on the internet one day, so the service we provide to customers is to make sure their assets are secured.

00:08:01 TPR1

Also, customers come from all over the world, right? So, we still need to comply with local regulations. For example, like the GDPR in the UK, although the UK has left the EU. For example, in our industrial computers, the products are intended to be located in strict and demanding environments, such as military applications like submarines, tanks, and warships. Therefore, the service we must provide to customers is to make sure these assets are secured.

00:08:41 Interviewer

So, what are your main customer sources? Are they from certain regions or industries that account for a larger proportion of your business?

00:08:52 TPR1

We have customers from various industries because we have several Business Units (BUs). For example, we have the Medical Product BU. In this BU, we provide products for the medical industry. For instance, when you see hospitals promoting large equipment like Da Vinci surgical systems, X-ray machines, or MRI machines, they all require computers. These high-tech computers fall under the category of industrial computers. Additionally, we also cater to the Defense BU, which includes military applications. For example, we provide computers for missile guidance systems, tanks, and submarines. These military-grade computers are also part of our business scope.

00:09:25 TPR1

So, as I mentioned earlier, in the context of defense, for example, the U.S. Department of Defense has the Cybersecurity Maturity Model Certification (CMMC), and Taiwan is currently making efforts to adopt this system. Taiwan is developing its own defense industry supply chain, following the guidelines set by the CMMC. They are about to release version 2.0 to ensure compliance with future requirements. Compliance with the CMMC is crucial for companies that want to enter the U.S. defense industry supply chain. Fortunately, we have a subsidiary in the U.S., and as a vendor under the U.S. Department of Defense, we are positioned further down the supply chain as a supplier of goods.

00:09:52 TPR1

Because we may supply products to intermediate vendors who conduct business with our Ministry of National Defense, we may be required to comply with regulations such as CMMC (Cybersecurity Maturity Model Certification) and GDPR (General Data Protection Regulation).

00:10:08 Interviewer

I see. So, it sounds like you also have some collaboration with government agencies.

00:10:16 TPR1

We must follow what the government agencies require, but it can be quite exhausting.

00:10:24 Interviewer

Okay, let's move on to the third question. So, what is the main reason why your customers typically seek your services?

00:10:36 TPR1

This part is more related to the business and sales aspects. I think customers seek [a private company]'s products because they meet their requirements, whether it's in terms of function or price.

00:10:47 Interviewer

For example, which part of the function do you think customers are more concerned about?

00:10:53 TPR1

I'm not sure because I'm not in sales, so I don't really understand this part.

00:11:01 Interviewer

Okay, no problem. Let's move on to the fourth question. Which part of network security do you think most customers have less understanding or knowledge about, and which part they need support from you?

00:11:19 TPR1

I think they are all just ok…. less understanding…..

00:11:24 Interviewer

Or maybe they lack something. Because they lack something, they hope to find you to support them.

00:11:34 TPR1

Because we are not a security provider.

00:11:37 TPR1

Yes, that's right. To answer this part, from our perspective, we do have lower-tier suppliers. For instance, when we produce a motherboard with many components, we still need to work with vendors at the lower level. In this case, when customers request certain standards or certifications, such as the supply chain security or the Trust Supply Program (TSP), we have to audit our lower-tier suppliers as well as the vendors we work with to ensure compliance.

00:12:07 TPR1

If the question is framed this way, then I can answer it.

00:12:13 Interviewer

Okay, then let me rephrase the question.

00:12:24 TPR1

If the question is framed in the way I just mentioned, then I can answer it. Is that okay with you?

00:12:27 Interviewer

Sure, that's okay. As long as it is like that.

00:12:29 TPR1

Well, based on this, most of our vendors face a resource shortage. Our vendors below us must even have more shortage. If we are a small or medium-sized enterprise, then most of our partners are probably small enterprises, and they have invested less in cybersecurity resources compared to us. So, I think the main issue we face is the shortage of cybersecurity resources, whether it's in terms of human resources or cost. Can I answer like this?

00:13:03 Interviewer

Yes, that's a good answer. In Taiwan, we generally lack resources in various aspects of cybersecurity.

00:13:13 TPR1

Because business owners may feel like they are spending money without seeing any benefits, like...

00:13:20 Interviewer

Yes, that's right.

00:13:22 TPR1:

It can be said that investing in cybersecurity is like insurance. You pay for insurance every month, but you never know when you'll need it. So for most business owners, they think, "Oh, let's wait until something happens before we do anything." For example, I may have been running my business for 20 years, but if something happens, even if it's just once, the cost I'll have to pay in terms of money and time might still be less than the insurance fee I've paid for 19 years.

00:13:48 TPR1

So, in this case, we can't blame the companies because it's a mutual relationship between the upper and lower tiers. From the perspective of a company, you can also understand this approach. Therefore, if you want to improve the overall cybersecurity of an enterprise, it's like joining NATO. When you join NATO, you must allocate a certain percentage of your GDP to defense, it's a standardized requirement. Similarly, if the government implements a concept like this, where companies going public must invest a certain percentage of their profits in cybersecurity, it becomes a necessary requirement. Otherwise, it would be considered illegal or problematic. With such government regulations in place, companies will truly invest in cybersecurity.

00:14:32 TPR1:

But as I just mentioned, NATO, how many members fail to meet the standards even though it's established? Germany has recently been in the news saying they need to work harder to meet the standard, right?

00:14:42 TPR1

So, you see, even the requirements set by organizations like NATO may not be strictly enforced from the perspective of NATO member countries as individual nations. So, if you don't approach this from the government's standpoint, it becomes an even more challenging task.

00:14:54 Interviewer:

From my understanding, most businesses are reluctant to invest money in cybersecurity.

00:15:07 TPR1:

They're not necessarily reluctant. They might think, "I know there's a risk here and if my business gets attacked, it could be destroyed. I'm sorry, I really can't invest right now." But this is the information we receive from the employees, but behind the scenes, is it really like that? Well, we are not the board of directors, so we actually don't know what the real reasons behind it are.

00:15:29 Interviewer

Yes, exactly. Nowadays, many companies tend to emphasize that the whole board of directors in the company, should take a supportive stance towards this issue. This way, the company will pay more attention to this aspect.

00:15:46 TPR1

The law is being amended recently, and in the future, at least one of the directors of a company should have a background in cybersecurity.

00:15:50 Interviewer

OK, that's great. Then let's move on to the fifth question. But is it not suitable for you here?

00:16:03 TPR1

If you ask from my perspective, because I am in charge of the cybersecurity office and the information technology department, all the network attack issues will come to me for handling. If you want me to answer from the perspective of my handling, I can still do that.

00:16:19 Interviewer

Yes, then let's hear your perspective.

00:16:21 TPR1

Uh, the most common form of attack, well, currently, it would be phishing emails, because it's something that users can easily fall for. However, if it's discovered by our own technical personnel, it could be injection attacks. They might use any type of injection to break in, gain the highest privileges, and then establish what we call a "parlour" or a sort of cybercafe on the machine itself, essentially creating a network-like concept between our server and the hacker.

00:17:04 TPR1

This is currently the most common form of attack. For protection, we employ various measures such as, for example, layer 7 firewalls, SOC (Security Operations Center), and many other protective mechanisms.

00:17:18 Interviewer

Hmm, okay. So, can you briefly talk about your main protection mechanisms?

00:17:28 TPR1

Well, we have an NG firewall for our internal and external networks.

00:17:35 TPR1

Have you heard of an NG firewall?

00:17:36 Interviewer

No.

00:17:37 TPR1

Its full name is "Next-Generation Firewall," which is currently one of the most advanced types of firewalls. As we know, a firewall is used to block or analyze traffic. In the past, we had the OSI model, which consists of seven layers, including the network layer. Traditional firewalls operated at the third layer, which is the IP layer, where they could block or allow traffic based on IP addresses and protocols. However, the so-called Next-Generation Firewall (NGFW) can analyze traffic at the application layer, making it capable of making decisions based on specific applications.

00:18:09 TPR1

For example, between you and me, the traffic is actually unsecure. If I make such a judgment, there might be an issue. However, with behavior detection, this generation of firewalls can provide us insights into things that are not visible to the naked eye. That's the first point. The second point is about endpoint protection. The old approach used to be pattern scanning, where features are identified after an event has occurred and been analyzed. But now, we also employ NDR (Network Detection and Response) or SDR (Security Detection and Response). These methods focus on behavior detection and judgment. For instance, we mentioned encryption earlier, which is a type of behavior. Therefore, modern endpoint protection is more advanced and expensive. It can assess whether your behavior is abnormal and, if so, forcefully terminate it. Just like WannaCry and Covid-19, malware can spread laterally. With higher-end endpoint protection, if it detects that a system is infected, it will immediately isolate it.

00:19:16 TPR1

So even if there is a WannaCry infection in the same local network, if it is detected and isolated, others will not be affected. Therefore, many more advanced techniques are needed to protect enterprises now.

00:19:32 Interviewer

I understand.

00:19:34 Interviewer

Let's move on to the sixth question. Earlier, you mentioned that you have some forms of handling network attacks. So, if, for example, you receive a network attack that has already breached your defense line, I believe the company will have some ways to reduce the damage and handle the situation. Can you briefly explain these mechanisms?

00:20:01 TPR1

In cases like this, regarding policy matters, since we have implemented ISO/IEC 27001, there are relevant policies and requirements for information security incident management. This is crucial, particularly for having a PSIRT (Product Security Incident Response Team). When you encounter security incidents, you need to manage and mitigate damages effectively, and this requires proper policy planning in advance. Otherwise, when the incident occurs, you may not know what to do, and that becomes a significant problem. As for mitigation, our approach is currently based on SOC (Security Operations Center).

00:20:38 TPR1

SOC stands for Security Operation Center. Typically, in regular enterprises, only companies like TSMC or financial institutions might have their own SOC. However, our SOC is outsourced. We use an engine-based approach where we install the engine on our core machines, allowing all machine logs to be sent to them 24/7. They have a dedicated team that continuously monitors and helps us address any security issues.

00:20:52 Interviewer

OK.

00:21:09 TPR1

As for management, we need to rely on internal management mechanisms.

00:21:13 Interviewer

OK.

00:21:18 TPR1

The last step is calling the police.

00:21:21 Interviewer

Yes, yes, yes, call the police, because actually, based on my reading of some literature, my understanding is more on the literature side. Many antivirus software or security solutions are more capable in defense, but when facing network attacks, they sometimes cannot respond well.

00:21:55 TPR1

What you are asking now may be about identification, that is, when you are attacked, you need to track back afterwards.

00:22:31 Interviewer

That's one aspect, but what I'm talking about now is during the attack. Because many times you may be doing defense, and the defensive part may become, I am only doing defense before the attack.

00:22:33 Interviewer:

I feel like it's a bit like Covid-19. It's like Taiwan's initial strategy for Covid-19. I used this metaphor to tell my supervisor, and he thought it was quite interesting. Initially, when Covid-19 started, Taiwan was very alert because we had experience with SARS before. So everyone started calling for wearing masks, and everyone wore masks obediently. Maybe in the UK and other countries abroad, they didn't care about wearing masks. Then it became that the epidemic in foreign countries became very serious, and it had already attacked. Taiwan protected itself very well, and the virus did not attack. There may be a few cases that got in occasionally, but in the long run, if it's short-term, I think it's effective. But when it's long-term, for example, it may last for several years, Taiwan cannot sacrifice its economy for Covid-19. You still have to cooperate with other multinational companies, and you cannot always restrict certain numbers. Then it became that, hey, we may gradually relax, and when the attack comes in, our confirmed cases skyrockets, and then we start...and Taiwan did not advocate for getting vaccinated at first. I can describe getting vaccinated as a more active defense method. Foreign countries actually advocate it more at the beginning, but Taiwan did not. Taiwan advocated wearing masks at the beginning, and at the beginning, the vaccine was not widely promoted. Then it became that when the virus breached your defense line, Taiwan suddenly collapsed. So, we started from May 2021, and at that time, it started to become serious. It took some time to gradually ease, but of course, I think Taiwan has done well compared to foreign countries. It's just that what I mean is that there is a kind of similarity with cyber attacks.

00:24:16 TPR1:

The same meaning, because in cybersecurity, we understand that we often talk about prevention.

00:24:21 TPR1

It means we need to be proactive in protecting ourselves. This protection involves considering potential incidents during the design or product selection phase. If we look at it from the perspective of businesses and governments, just like dealing with Covid-19, should I buy so many vaccines right from the start? Will the investment be worth it in the end? Many businesses and governments approach things in this manner. Although it might sound straightforward, some business owners tend to wait until an incident occurs before taking action. Why is that?

00:24:53 TPR1

Because when incidents happen, businesses will cry as it affects their revenue, and their factories might face interruptions. The government will also cry because public grievances will rise, and they can't afford to bring the economy to a halt and face a recession. So, this is very realistic.

00:25:09 Interviewer

This is very realistic.

00:25:10 TPR1

So, for prevention, you must first do proper planning. We all know that, but to be well-prepared in the end, you must invest a budget and manpower, right? So, in fact, I think what was mentioned earlier about the vicious circle is ultimately an unsolvable problem. Not every company is like TSMC.

00:25:34 Interviewer

Okay, now let's move on to the seventh question. And for the seventh question, you just need to answer as much as you can, and it's about the network resilience of the technology services you provide. How is it?

00:25:52 TPR1

Network resilience? It's actually the first time I've heard of this term. What does it mean?

00:25:57 Interviewer

It's like, um, how should I put it? It's called "resilience" in English.

00:26:03 TPR1

If you don't know how to describe it, that's not good.

00:26:06 Interviewer

It's like when you are under attack, for example, your network is already attacked and paralyzed, then you must have some backup plans to temporarily restore it so that you won't be completely paralyzed and the whole company can't function.

00:26:31 TPR1

In terms of cybersecurity, this is called disaster recovery. Disaster recovery comes in various forms, and cybersecurity is just one of them. For example, there are disasters related to power outages, fires, nuclear explosions, which are all part of disaster recovery. So, to have effective disaster recovery, you need to plan a proper backup strategy and conduct restoration drills.

00:26:51 TPR1

The things you backup, you must have planned and regularly done restore, verification, and testing. Otherwise, when an incident occurs, if we need to rely on backups and they are not reliable, wouldn't it be worse? Yes, our company's reputation is good because we were aware of the WannaCry incident in 2016, and we knew that it was a sign of future threats. We understand that cybersecurity breaches are inevitable for any enterprise. With this awareness, we have been gradually fortifying our defenses and implementing design plans, such as daily differential backups and weekly full backups in [the name of city A]. Additionally, we perform offsite backups to a data center in [the name of city B]. So, if there is a problem in [the name of city A], we can simply drive to [the name of city B], bring the servers back, and copy them online.

00:27:57 Interviewer

Do you think there are different types of risks for cloud and local? Many people think that the cloud is also a high risk, although it is very convenient, but the risk is also high. What is your opinion?

00:28:14 TPR1

Let me tell you, there are some bosses in Taiwan who don't understand, they will think, let's just use the cloud, it won't be hacked because the probability of the cloud being hacked is lower. But he actually overlooked one thing, the cloud is divided into different types. Have you heard of IaaS? You can look it up later.

00:28:34 Interviewer

No.

00:28:40 TPR1:

There are IaaS and SaaS in the cloud, and IaaS stands for infrastructure-as-a-service.

00:28:41 TPR1

It means that your infrastructure extends beyond its original location. Instead of renting a server cabinet in a data center, you might have shifted this role to cloud services like AWS or Microsoft Azure. Since these cloud platforms have physical machines that you can manage remotely, they operate in the cloud. However, there still needs to be connectivity between your enterprise and the cloud. Otherwise, how would you manage it? So, even with this extended setup, there's a possibility that one of the cabinets in your data center, for example, could still be compromised or encrypted. Let's take another example, a SaaS (Software-as-a-Service) part of your infrastructure. Services like LINE, Microsoft Teams, or web-based video conferencing tools like Zoom are examples of cloud-based SaaS services that you can't maintain directly.

00:29:37 Interviewer:

Hmm, I see.

00:29:39 TPR1:

Like the more common examples, such as Slack or Salesforce, they offer additional services purely in the cloud. From an IT perspective, for certain endpoint devices, you cannot perform remote operations because they are entirely GUI (Graphical User Interface) based. In such cases, enterprises may need to access their data through web services and make API calls. This setup minimizes the risk of attacks because the operations cannot be directly accessed, thus avoiding token-related vulnerabilities.

00:30:08 TPR1

Compared to IaaS, the risk of SaaS is relatively low.

00:30:11 Interviewer

Thank you for providing a lot of information.

00:30:17 TPR1

If you have any questions later, feel free to consult me. I am a more enthusiastic zodiac sign when it comes to helping others.

00:30:20 Interviewer

Oh, okay, thank you.

00:30:28 Interviewer

So let's move on to the eighth question. It may be a bit sensitive, but I wanted to ask, what do you think is lacking in the technology services provided by your company? And how can it be improved? Maybe we can answer this together for questions eight, nine, and ten. So, um, because nothing can be perfect, right? Which aspect do you think needs improvement, and do you have any plans for the future?

00:30:59 TPR1

This question, for me, becomes two different aspects. The first aspect is the core deficiency, which is very crucial when it comes to management. If the management doesn't stand behind certain aspects, such as updates to cybersecurity policies, it becomes challenging to implement changes. For example, I know cybersecurity policy updates can be done quickly or policies can be set up globally for thousands of people. However, if the management doesn't step forward and provide support, it becomes difficult to implement these changes because each culture is different. Especially for a global company like ours, with operations in Germany, the UK, the US, Japan, Singapore, and more, it's challenging to have a policy that satisfies everyone. Changes in cybersecurity policies often require significant effort and can be inconvenient in terms of budget.

00:31:29 Interviewer

I see.

00:31:49 TPR1

For us, with an IT security background, this is something we should do. So, it becomes quite a dilemma if the management doesn't provide support or if they lack the know-how to support us. When we bring up these issues, they may respond with a vague "yes" or "okay." This kind of response can make it difficult to move forward to the next steps.

00:32:11 TPR1

So, I feel the inadequacy lies in the way companies, including our own, approach cybersecurity. For example, as we mentioned earlier, when it comes to planning and designing cybersecurity measures, if you read books, research papers, and stay updated with the news, you will know what needs to be done. It's clear in the minds of cybersecurity professionals what actions to take. However, the first issue is with the management; if they don't provide the necessary resources and leadership, and the second issue is the lack of budget and manpower. Without these, it becomes challenging to establish a comprehensive cybersecurity program.

00:32:43 Interviewer

Yes.

00:32:46 Interviewer

What about the first and second aspects you mentioned earlier?

00:32:52 TPR1

The second aspect is the technical level. Purely technical aspects include software, hardware, and training. I think training will be the key. As I mentioned earlier, you need to improve the security awareness and expertise of your employees.

00:33:10

OK.

00:33:12 Interviewer

So, do you think your company or your department will propose some improvement plans for the shortcomings you mentioned in the future?

00:33:24 TPR1

Yes, because in reality, the foundational technical aspects, such as hardware, advanced firewall, and endpoint protection, are well-established in our company. We have a good backup system in place as well. So, if we were to rate ourselves on a scale of 1 to 10, we would probably score around 6, 7, or 8 in terms of hardware and design aspects; these are not major concerns. However, I feel that our training programs are weak. Training is crucial and requires involvement from everyone, including me in my role and all the other members. Last year, we completed the implementation of ISO/IEC 27001 certification, and as a result, education and training became an essential part of our Information as a Service (IaaS). I am personally committed to promoting education and training and providing support in this area.

00:34:12 TPR1

Actually, a company wouldn't just implement these certifications for no reason unless you are an e-commerce company, you might need it. For manufacturing companies like us, there is only one possibility, which is customer demand.

00:34:31 Interviewer

Yeah, customer first.

00:34:35 TPR1

So our motivation is always the government first, and then the customers. It's hard to do something voluntarily, it needs a trigger.

00:34:47 Interviewer

It also requires investment in time and money.

00:34:50 TPR1

Because, for example, in your department, your immediate boss might understand these matters very well, and he knows what should be done. However, will the higher-ups agree with your perspective? Not necessarily.

00:35:01 TPR1

So, if you think from a business perspective, does it make sense or not? Government requirements, I have to do it; customer demands, I have to do it. So now, replacing the company becomes a matter of necessity, and that's when security gets approved.

## Section G

00:35:18 Interviewer

Now we come to the last section, the G section, which is about collaboration between the public and private sectors. The first question is about your opinion on such collaboration in terms of cybersecurity. Do you think it can really contribute to the development of cybersecurity?

00:35:37 TPR1

Taiwan is making progress, but I think the progress is still limited.

00:35:48 TPR1

For example, in our national military, when they are looking for information security-related positions, they set some requirements that may seem funny to those who understand cybersecurity. For instance, they may ask about age or university education, but for someone who truly understands cybersecurity, the key factor is their technical knowledge to protect the country from cyber attacks. Asking about age or education doesn't really make much sense. However, I can see that the public sector is making progress. In recent years, there has been a regulation,….but I forgot which law or provision,.. that allows businesses to deduct cybersecurity expenses from their taxes.

00:36:40 Interviewer

Oh, I see. They can deduct it from their taxes.

00:36:42 TPR1

You can go online to check the relevant news. I forgot, but it seems like this year is the last year for that. There is a government program with a nice slogan as they always have, but for me, the program is not bad, it's just that the tax deduction amount is too small.

00:36:55 TPR1

So, for business owners, they don't have any incentives. And then, for example, for us to establish Ministry of Digital Affairs, there should also be opportunities.

00:37:09 TPR1

And there is also TWSEC in Taiwan, have you heard of TWCERT?

00:37:13 Interviewer

No, did you just mention Ministry of Digital Affairs or something?

00:37:16 TPR1

It's Audrey Tang's Ministry of Digital Affairs. Our future is in her hand.

00:37:20 Interviewer

I see.

00:37:22 TPR1

The future of the Ministry of Digital Affairs is in its own hands, because our president Tsai Ing-wen last year,… every year ITM (International Trust Machines Corporation) holds a cybersecurity conference and we also attend it. They came up with the slogan "Cybersecurity is National Security" a few years ago.

00:37:39 Interviewer

Yes, I saw that news.

00:37:39 TPR1

And they talk about it every year. So it is actually making progress, but you know our government is like this.

00:37:45 TPR1

And TWCERT is Taiwan Computer Emergency Response Team.

00:37:49 Interviewer

Oh, I know it.

00:37:53 TPR1

TWCERT has been doing well in recent years. After joining TWCERT, they will provide references from government agencies or enterprises with captured intelligence on a daily basis. Upon receiving these references, we take the next step of action, which is to confirm and implement the corresponding prevention measures. Since we already have the intelligence, why not block it? Although it may require additional effort from our personnel, it's better to be proactive. Not only TWCERT, but there is also the CISO Alliance, which is Chief Information Security Officer (CISO) Alliance.

00:38:26 TPR1

But this one, it's not part of the government, it's considered a corporate foundation, so should I mention it?

00:38:33 Interviewer

Oh, you can share it, sure.

00:38:47 TPR1

The other one is the Taiwan Chief Information Security Officer (CISO) Alliance. In this case, they regularly gather the cybersecurity directors or members who are part of the alliance and hold periodic briefings on global trends and developments. This is a private organization, while TWCERT is a government organization, indicated by its .org.tw domain name.

00:39:14 Interviewer

Okay, so overall, you think that cooperation between the public and private sectors is the right direction for cybersecurity?

00:39:24 TPR1

Definitely, it has to be that way.

00:39:32 Interviewer

Definitely, definitely, definitely. It's just that maybe it's not mature yet and still in the early stages, but it's moving in that direction in Taiwan, right? Okay.

00:39:33 TPR1

Like I mentioned earlier, the US Department of Defense's CMMC, Taiwan is also calling for it recently, and calling for this area.

00:39:44 Interviewer

Actually, Taiwan and the UK have quite similar overall strategies in terms of cybersecurity. What I mean is that countries like the UK, the US, and Taiwan are more proactive in their defense strategies, rather than passive. This means that, for example, countries like Germany - I forget, it might be France, Spain, and Germany - are more passive in their defense strategies, meaning that they only take action to defend themselves once an attack has occurred. But with a proactive defense, it's possible to target and destroy a threat before it becomes a problem.

00:40:18 Interviewer

Taiwan, the UK, and the US are all moving in this direction, which is different from Germany and Spain, for example. So I think that's quite special.

00:40:29 TPR1

Another thing is the defense industry chain in Taiwan.

00:40:29 TPR1

Our company is also one of the alliances with the government. If you look at Japan and South Korea, for example, they have been doing this at the national level for a long time, because they have their own military capabilities - they make their own tanks, missiles, and planes. If they can do it themselves, of course, they want to join the US defense industry chain, so they adopt the CMMC system used by the US, just like Taiwan does, and implement it locally with government support. CMMC is completely related to cybersecurity requirements.

00:41:04 TPR1

This is the government.

00:41:06 Interviewer

So, is it the defense industry chain in Taiwan?

00:41:09 TPR1

Yes, the Taiwan Defense Industry Development Association.

00:41:14 Interviewer

Yes, yes, I see.

00:41:15 TPR1

The other one is the Cyber Security Management Act.

00:41:17 TPR1

The Cyber Security Management Act is a recent government regulation. This act requires that when government-related agencies make purchases, their suppliers and supply chain must meet information security requirements. For instance, we have collaborated with Academia Sinica. Do you know what they are doing in Taiwan?

00:41:34 Interviewer

Academia Sinica, I think…

00:41:38 TPR1

Academia Sinica is involved in missile development, which makes it subject to both national defense and information security requirements. In the government's Cybersecurity Management Act, it stipulates that if you want to participate in government procurement, it is categorized into different levels based on your compliance with information security requirements. These requirements are divided into information and management categories, such as management and technical. For the management category, you need to comply with certain standards, like ISO 27001, with specific versions such as the 2022 version. In the technical category, it may require certifications like Cisco CCNA or other vendor-specific certifications. To bid for these government projects, your company's personnel must possess these certifications, whether in the management or technical category, as per the government's requirements and leadership.

00:42:20 Interviewer

Okay, let's move on to the second question. Earlier we talked about your views on the concept of national cybersecurity. Now, in terms of cybersecurity in Taiwan, do you know if there are any collaborative mechanisms or experiences between the public and private sectors?

00:42:42 TPR1

I already talked about that earlier.

00:42:44 Interviewer

Yes, you did.

00:42:48 Interviewer

But in your opinion, are there any areas in which these collaborative mechanisms could be improved or where they are lacking? Or do you think there are areas that could be developed for better collaboration?

00:43:00 TPR1

In what directions…..

00:43:05 TPR1

I think it would be what I mentioned at the beginning, which is providing education and training to the public. By joining TWCERT, a government unit, it includes many cybersecurity responses. You can find relevant information about these by searching online, but only IT professionals or those knowledgeable about cybersecurity would pay attention to these matters.

00:43:32 TPR1

You think like this, for example, when Covid-19 first started, government officials like Audrey Tang or Premier Su Tseng-chang, they would post some meme images on their Facebook pages, right? When have you ever seen Taiwanese politicians make a cybersecurity-related meme image?

00:43:50 TPR1

Never, so the propaganda aspect is really lacking.

00:43:52 Interviewer

Relatively lacking.

00:43:55 TPR1

So national security can't rely solely on IT professionals.

00:43:58 Interviewer

Maybe we need to use more social media so that the public can be more exposed to it.

00:44:06 TPR1

Right, right.

00:44:08 Interviewer

Yes, so in your perception, do you also feel that the general public's knowledge of cybersecurity in Taiwan is still insufficient?

00:44:14 TPR1

Very weak, well, I think this might be an issue for governments in every country. Look, for example, scams—no matter what type of scam, whether it's an online scam or phone scam, it's related to cybersecurity. So, phone scams and internet scams are different, but they both fall under the category of scams. If people are already aware of these scams and know that they are scams, then why do so many still fall victim to them?

00:44:41 Interviewer

Hmm.

00:44:44 Interviewer

Because scamming methods and techniques are constantly evolving.

00:44:50 TPR1

That's similar to the concept of phishing emails.

00:44:58 Interviewer

Okay, I think that's about it.

00:45:05 Interviewer

Okay, we'll end it here. Thank you.