Ways to Work: Episode 1 — Cyber

[MUSIC PLAYING]

JENNIFER TIANG: Cyber criminals, these are the really prevalent cyber risks facing organizations today. And the risk is that we're all grappling with the change to remote working.

VOICEOVER: Welcome to "Ways to Work," a Willis Towers Watson podcast series exploring the modern workplace through the lenses of people and risk with a focus on the Philippines and the broader Asian market. We offer HR and risk professionals at every level in every industry, access to current thinking on topics that matter most to employers and employees.

JOAQUIN UY: Good afternoon, ladies and gentlemen, welcome to this episode where today we're going to be focusing on a topic that's very important to the environment that all of us are operating in nowadays because of COVID-19 and the changes that we've had to introduce to our working arrangements. My name is Joaquin Uy, I'm the Deputy Head for the CRB segment here in the Philippines, and I'll be your host for today's episode.

It goes without saying that the threat of cyber risks has definitely been heightened, and the thing about it is that even prior to the pandemic making its full effects felt, we've seen an increase in the number of threats, hacking incidents, ransomware, so on and so forth, and all of these seem to have gone up a notch. And for the next few minutes, we're going to be speaking about the threat of cyber risks, what we've been seeing from a threat environment in the, not just from a regional, but also from a global perspective, and take time to think about practical ways where all of us can protect ourselves and mitigate these sort of risks.

I'm joined by none other than our regional lead for cyber risk in Asia from Willis Towers Watson, Jennifer Tiang. Jennifer holds the distinguished privilege of wearing two hats. She's worn an underwriting hat, and now she's in the broker side of the insurance business. Jennifer, good afternoon. How are you doing?

JENNIFER TIANG: Good afternoon, Joaquin. Very well. Thank you. Really great to be here with you this afternoon.

JOAQUIN UY: Thanks a lot for making time and agreeing to join us today. Take me to the day that Singapore or its government basically announced that the circuit breaker was in place.

JENNIFER TIANG: Yeah. Oh, gosh. It almost felt surreal. I remember we had a phone tree, a corporate text messaging system, that was a way for all of management to notify us immediately what to do. And I remember receiving the text, and I just thought, what? And a silly thought I had was, oh, my gosh, my plant in my office, it's going to die. I'm not going to get back to it.

But they had been telling us for a couple of weeks to bring our laptop home every day, so we were at the ready to resume work from home. And so you did that every day, and then one day, it did appear, yes, you will be not returning into the office. And it's really like the rug being pulled out from under your feet. You took for granted your everyday routines, like going to the coffee shop, going to see your colleagues. And then so to (immediately then) work from home, it just seemed very unceremonious and very abrupt, like you said.

But one situation I can recall, after our first circuit breaker, when there was a little gap between a second circuit breaker. But in that gap, I actually moved house. Moving house, I had to get my laptop, and my (VPN) connection reconfigured in a certain way. But when I moved into my new house, it wasn't possible to be configured and I was trying to get access to our IT people.

I think it was a day and a half where I had no connectivity. And I remember thinking, wow, this is really hitting home. How reliant we are on connectivity, and I was really stressed. There were urgent client deliverables, I had to be on meetings, so these had to be conducted via my phone. I'm very aware of cyber risk, but this was me living it, I suppose. This was me not having for more than 24 hours access to our VPN, to our network drives, access to client files. And it was really disruptive, very stressful. And I just thought, wow, imagine this on a large-scale basis. Imagine this for 200 colleagues in an organization.

We're really so reliant on our IT teams. I think they're the unsung heroes as well of this remote working shift. They're working double time, triple time, trying to meet all these IT service helpdesk notes. Also, trying to make sure that the business is conducted in a secure way. So I think, yeah, we really should give a hand to our IT teams.

And I just thought, wow, the fate of organizations really in this time is carried more or less by IT teams. In prior times, there were perhaps other workarounds. But we cannot overstate how important they are for that seamless kind of operation. That was a real lesson for me when we went to our second circuit breaker.

JOAQUIN UY: And I guess, we can both agree that in some ways, our IT support teams are also frontliners in this battle.

JENNIFER TIANG: Oh, absolutely. I'm sure all of us at one point have had to reach out to our IT team to sort out something. Even after you read all the documentation and try to help yourself, at some point, we've had some help from our IT teams.

JOAQUIN UY: I know that we've seen a tremendous amount of change. And as we rely upon technology in a far greater way because of COVID-19, because of restrictions to mobility, and because we want to make sure that services are provided in a seamless manner as possible, we've also seen that it comes with an exchange. From what you've seen over the last year and a half, what have you observed to be the greatest threats to a business from a cyber point of view?

JENNIFER TIANG: Really good question. I think everyone's going to agree that the last year and a half, it's just completely upended all our kind of notions of business as usual. But I think, like you mentioned earlier, even before that, there was an increasing understanding of how reliant we were on technology and connectivity. We have such a reliance on data and systems (to actually carry out work) that you could kind of think of this move to remote working as the largest global en masse digital transformation project the world has seen.

I heard that the move to remote working a year and a half ago from every country brought forward IT (digital transformation) roadmaps; it shortened them by five years, seven years. So it really pushed everything ahead of what might have been in normal times, two-year, five-year IT digital transformation rollout. In terms of the most significant threats, it really has been the fact that we've got very opportunistic and sophisticated and very intelligent and smart commercial ransomware groups – or not even ransomware groups, though they are the most frequently kind of flagged up by threat intelligence our clients see, but cyber criminals – these (their activities) are the really prevalent cyber risks facing organizations today.

And the risk is that we're all grappling with the change to remote working. We're a year and a half in now. So hopefully, systems and protocols have more or less bedded in. But there are still open vulnerabilities. Colleagues are still quite dislocated from each other. And IT teams are dislocated from the rest of the organization. Everyone's working in this remote working environment. And so in this kind of “business as unusual” environment, it does open organizations up to more pervasive threats from these cybercriminal groups.

And the frightening thing is that, I'll just take ransomware as an example, they're making a lot of money. It's increasingly lucrative to be partaking in this kind of cybercrime activity. And we're all asking, how has this risen to such, almost epidemic levels. The rates of losses and notifications that I know insurers are sharing back to us are pretty frightening. They're saying they receive notifications daily or weekly. How has it risen so dramatically?

It’s almost like there's a perfect storm in terms of ransomware. And just to recap for the listeners, ransomware, very simply, is malware that is deployed on systems to encrypt them. And so you are, in

effect, held hostage by a ransomware group until you pay the amount that they are demanding. And then they'll send the decryption key to have access to your networks or files again. So it's that kind of extortion activity.

And it's been a perfect storm in a way because of the rise, well, on the one hand remote working, and on the other hand, also the rise in cryptocurrency, an anonymized, not untraceable – technically, it is traceable, but extremely, extremely difficult to trace and subject to heavy cryptographic tools to make it very, very hidden. So the rise in that makes it almost like a perfect vehicle to carry out these extortion activities.

Before, in the absence of cryptocurrency, cyber criminals would have many other steps to go through to try to hide or mask the funds being transferred, like opening up a bank account. And the world has gotten very strong at KYC measures and things like that for currency that is recognized by governments. So when you've got something like cryptocurrency that is outside of the government remit and not subject to perhaps the same oversight and regulation, there you have a perfect kind of money mule. So that's been an interesting trend we've seen.

JOAQUIN UY: You shared a bit about ransomware, which is certainly a topic in its own that I would like to touch on for today. Undoubtedly, one effect that this has had on us, and this is still somehow related to the threat of cyber risk is that the human connection has been missed a lot. Here in Manila, I look forward to seeing clients, speaking to them, and being with them personally, and obviously, that's been curtailed very significantly.

I've had one face-to-face meeting in the last year and a half, and I remember telling my colleagues about this, and I said that, number one, it felt great to be out. And number two, it felt great to actually be in front of a client. A few years back, we actually came up with this study that a very significant portion of cyber risks was born of the human side of the business, meaning employees are the highest sources of risks.

JENNIFER TIANG: Yes. Yeah, I think, if I recall correctly, it was 66%.

JOAQUIN UY: Yes, correct, 66%, yes. So are you seeing that that is still the trend nowadays? Or has there been a change? Not necessarily because of the pandemic, but because as you rightly say, we're just so reliant on technology. Would share with us your views regarding that, Jennifer?

JENNIFER TIANG: Yeah. Yeah. I would say that trend is consistent today. And I believe, the human element of cyber risk is going to continue as long as it is us doing the work and having that interface with technology until the point we kind of get stood down for robots or AI. But I think that human element is a very, very key risk management consideration.

And this role as the regional cyber lead for Willis in Asia, I'm really lucky to speak to quite a few CISOs, and I always try to pick their brain. I want to learn more about how they're at the frontline of cyber risk. They're the ones tasked with overseeing the risk management practices and IT security for the

organization. I ask them, where do you even start? And they always say people, they are the strongest line of defense, but they're also the weakest link so you have that paradox there.

And so if you are constantly educating them and making them cyber savvy, just making them a bit more cynical about every email that comes in your inbox and being aware of something that doesn't look quite right. I know in this kind of remote working time and everyone's very busy, and we're trying to be very responsive so we act quickly on emails that reach our inboxes. But we need to have that balance, that need of urgency and responsiveness with being very aware of the threats of very sophisticated hackers creating spoof emails that look exactly like Joaquin's email coming into the inbox and looking completely legitimate, but in fact, being from a bad actor.

And then if we add that human element, we click on the link that's in the spoof email, and all bets are off. No matter how strong the IT security controls can be, there's always going to be that human interface. So that's been the key message that a lot of the CISOs that we work with have been spreading towards their staff. And it has to be a ground up approach. Anyone that has access to the network or access to email, which really is everyone in the organization, is a key line of defense, but also a point of vulnerability.

JOAQUIN UY: Now, I would imagine that through these phishing emails, and if an employee unknowingly clicks on an email, this could potentially-- or result of doing so could potentially lead to ransomware attacks penetrating the networks or the systems of company. What's important for clients nowadays is that they are aware of the coverage and limitations of a cyber insurance policy. I mean, the last thing, of course, that we would want clients to get the impression of is that this is the panacea for all the problems, all the concerns related to the cyber risks.

The cyber market is seeing some changes in terms of appetite, in terms of risk rating, and so on. A few years ago, when the product was launched here in the Philippines, and this was probably back in 2013 thereabouts, we were always being asked by clients, should we consider this? Should we buy this product for us? And of course, one consideration would be it really depends on the nature of your business and what you think, rather how you think this type of product would benefit you relative to how you operate.

And one thing that we would also say to them was, now would be the best time to purchase this because the costs are not as prohibitive yet. Given that the market is evolving, and if the client were to come to you and say, Jennifer, I need guidance on-- I know that I need cyber, but I need guidance. This would be-- how much the cost would be and the protection that I'm going to get? Not to put you in a spot, but what would your recommendation be if a client were to come to you with those concerns when they're at the point in their journey where they're evaluating the purchase of this type of solution?

JENNIFER TIANG: Yeah. Yeah. And I completely understand the clients. You have to really do a deep consideration because this is a new insurance spend. This is not budgeted. This is completely new to the risk management budget. And so for a CFO or the risk manager, of course, they need to be doing their homework. And it needs to be a very compelling reason why you're making this new insurance spend

because if you're answering to a board, it's not going to cut it just to say, oh, I saw a headline in the newspaper, and it recommended that cyber insurance be considered. So I completely understand. And we definitely-- I know our practice in Asia is definitely not to leap to the insurance part. We try to understand the clients where they're at in terms of their cyber risk.

So a lot of the time they may be heard from a board member saying, oh, you should look into cyber insurance. Or maybe it's just been something that's been tabled, and they want to explore it. So really it's for us to sit down with them and understand what is the amount of risk that you're facing. So exploring the kind of quantification, like what is your maximum possible loss in the event x number of data records that you hold were breached? Or x number of hours, what does x number of outage downtime mean to you? That might not mean that much if you're a retail store, a bricks and mortar retail store, as opposed to an e-commerce. Six hours of you not being able to access your networks might not actually mean that much financially for you. You may be thinking we can actually absorb that cost. (You have to go through all) these different questions because cyber risk is so dynamic and multifaceted. Unfortunately, it's not as easy as looking at a property schedule of values, saying, oh, this building is worth this much. So we have to ask a lot of questions and work with the different teams within the organization to really understand holistically what is the loss that you could be up for.

And then from there, the cyber market has undergone a change, and I think we have to understand the market change in the broader context. It's kind of seeing how the cyber market that we call it hardened. So in layman's terms, gotten more expensive. But we have to understand that in the broader context, that means that claims are being made, so that means the risk is there. And it means that policies are being called on, so insurers are paying out. So that is good. There is that silver lining, I guess. Even though the premium you pay now compared to the premium you might have paid five years ago is going to be higher, that's a response to the more active risk environment your business is operating in. So it is really all relative.

Cyber insurance really has to be there as the last piece of the puzzle. After you've made the adequate investments into your own front line. (For example), you've invested in multifactor authentication on all endpoints for corporate resources. That's a really key question a lot of insurers ask-endpoint detection software. There are various kind of baseline things that we can work with our clients on to make sure that they have, which is two-pronged.

So it's first of all, that getting to that baseline is helping them on a day-to-day basis of preventing the risk of a cyber event happening to them. But then also, it's making them more insurable. So the insurer terms that will come after they've invested into their in-house IT security then transferring that residual risk to the insurer is going to be a lot more competitive. I think we're moving away from a transactional insurance approach, I suppose, to a lot more of a dynamic and more advisory focused one.

JOAQUIN UY: Well, it certainly has been a very insightful afternoon, Jennifer. And I thank you for sharing your time with us, your expertise, and your knowledge. I'm pretty sure that our listeners have taken away very important lessons from this episode.

JENNIFER TIANG: Great. Thank you so much. Thanks, Joaquin.

JOAQUIN UY: OK. So thanks to all of you our dear listeners of the "Ways to Work" podcast. We're going to continue our conversations with our leaders and experts around the key topics on people and risk and what matters most to employers and employees in the modern workplace.

[MUSIC PLAYING] VOICEOVER: Thank you for joining us for this Willis Towers Watson podcast featuring the latest thinking on the intersection of people, capital, and risk. For more information, visit the Insights section of willistowerswatson.com.