Convenor - Maggie Leese (ABSIA): Hi everyone. I can see you're all just coming in now. We'll just give about 30 seconds a minute to make sure all your audio is connected and give some time for any last minute people to come in.

Alright, well I think we'll still have a few people joining us but we'll get started. Hi everyone, welcome to this webinar today. Just a few things happening on the screen. Obviously, welcome to the webinar. We just ask you to keep your video off and stay on mute for the duration of the webinar. If you want to ask a question, we'll be having a Q&A session towards the end of the webinar so just send a message through chat until then. And without further ado, I'd like to hand over to our Non-Executive Director of ABSIA, Ian Gibson, to welcome everyone and introduce our guest today who is Gergana Winzer from Unisys.

Presenter - Ian Gibson (ABSIA): Thanks Maggie. Welcome everyone.

I'd like to start the webinar by acknowledging the Traditional Owners of the lands in which we all meet today. We would like to pay our respects to them and their cultures and to their Elders past, present and emerging.

Now to move to the webinar today. I'd like to introduce Gergana. I've actually known Gergana for several years and she's a wonderful speaker so I'm sure we're going to be entertained today. She's currently the industry director of cyber security in charge of Australia and New Zealand at Unisys. Gergana comes with a strong account management and business growth background. She has a passion for business and complex problem solving. Her involvement in IT and security industry led her to be the president of the ICT chapter of the Australia India business council and many of you might remember her from there. ICICA, the Sydney board member and then more recently, the Australian Information Security Association committee member. Gergana is definitely a passionate advocate and thought leader for cyber security, I know that from the years that I've known her and she's also a strong role model for female leadership. She's been a keynote speaker and panellist in several industry related events and also leading conferences. So, today I'd like to welcome Gergana and I'll hand it over to you now. Thank you.

Guest - Gergana Winzer (Unisys): Thank you Ian. Thank you Maggie. Thanks everyone for having me today, it's definitely a pleasure. And yeah, we've known each other for a very long time Ian it is true.

I would like to start today's session with asking a couple of questions and I don't know how familiar you are with Zoom, by now I guess very familiar, but there is a button on the right hand side, especially if you're using a laptop, called reactions. So if you click on the reactions, you can choose thumbs up or applause button. And I would like you to put your thumbs up if you have heard recently about all the different hacks that are happening in the country and whatever is going on at a cyber level. Let's see how many of you have put your thumbs up, yeah perfect. That's exactly right, excellent.

So that is the case and for the ones of you who do not know me or have not met me, I have been in the IT industry for about 15 years now coming from Italy from enterprise resource planning and software as a service so I had to deal with problems similar with the ones you have to face on a daily basis as ABSIA members. And I have gone into cyber security because it is an industry that inspires me given the fact that it can allow organisations to protect people's data because eventually that's what we do, we look at protecting people's data.

I'm going to start sharing my screen now.

Convenor - Maggie Leese (ABSIA): You should be all good to share your screen now.

Guest - Gergana Winzer (Unisys): Excellent, let's see if that works. And introduce the topic of today for you all.

Slide change

Guest - Gergana Winzer (Unisys): So we have decided to talk about increasing cyber resilience because if you want to put it at a level of, you know, health for an example as an analogy. If we use health, what is really good when it comes down to resilience of our immune system is that if we have a resilient immune system no matter how many germs, viruses, bacteria attack us, we can very quickly recover. The same thing is valid for cyber. Whatever happens, if you're resilient, then you would be able to very quickly respond to the threats and then, as a consequence, recover. So hence, cyber resilience is an extremely important topic and again, a lot of organisations such as yours, to have a better way to respond and recover immediately after having suffered the cyber attack.

Slide change

Guest - Gergana Winzer (Unisys): Now COVID-19 has been obviously a very huge disruptor for many industries *inaudible* your industry. And it has created thousands of concerns for employees and changed the way we work. And that something, it's a phrase that I found from *inaudible* which says we weren't exactly ready.

So 68% of Australians were working from home during the initial part of the pandemic. Unfortunately we're now facing the second part. And 42% of Australian businesses expect to permanently maintain working from home workforce.

Why I'm sharing these with you when I'm sharing when we talk about cyber resilience and what that means to you is that you would be subject to all the threats and all the different issues that can arise by you having your employees working from home. There would be a single point of failure which is the VPN, which we all have been using no matter what's going on. And there will

be issues related to bringing your own device. Issues related with saving data on people's own devices etcetera etcetera but I'll dive into that a little bit more later.

The most important thing that I wanted to set the stage for you today is that you're going to learn a few practical, tactical but also strategic steps on how to build and maintain cyber resilience, which we have just established is a very important topic to have.

Slide change

Guest - Gergana Winzer (Unisys): So as a cyber presentation, we had to include a hoodie. We could not have missed having someone looking like a hacker wearing a hoodie, so this is the one. But why I'm sharing it is because cyber attacks will still happen and regulators will still regulate no matter what's happening with COVID and no matter what's happening with the industries all over the world. Those two things will keep happening and unfortunately for us in Australia …

Slide change

Guest - Gergana Winzer (Unisys): … There has been more and more cyber attacks happening over the past few months. More than ever before to the point where the Prime Minister, as you all agreed initially, has said to us that we have recently become a victim of cyber attacks, state-sponsored cyber attacks.

As you probably know and can connect to that, cyber attacks can be of two types. One can be malicious and for the purpose of making money or making profit for cyber criminals. And that the second one can be for collecting data or disrupting the systems of a certain country because they have been ordered, so to speak, by state-sponsored cyber attacks.

So I'm showing you a few logos here just to kind of bring the conversation to reality to what has been occurring in our country in the last few months. And again, I would like you to raise your hand or put your thumbs up if you're aware of any of those particular attacks or if you have read in the media about those attacks. Yeah, I can see a few people raising their hands. It's a real issue and it's still happening.

Slide change

Guest - Gergana Winzer (Unisys): So what is important to know and what is important to understand when it comes down to cyber resilience and also to cyber attacks. I've put together a couple of concepts and a couple of very useful tips and tricks for you to take home and if you want, you can take a note of those.

I saw somebody was asking before in the chat if we will be sharing this presentation, I have no issues to share the presentation with ABSIA team. And Maggie, correct me if I'm wrong, I can

send it to you and you can then share it with the rest of the participants in a way. That's not going to be a problem.

Inaudible

Thank you Maggie, thanks for that.

So diving into it, there are two important points. Number one, have I been hacked and number two if I have been hacked, how can I stop it. So in this case scenario, have I been hacked, comes down to three important steps that you can take in order for you to establish whether or not you have been hacked.

Number one happens to be do your research. Like everything, we have to do our own research and understand what threats are actually facing our own industry, facing our own organisation. There will be threats that are connected to people, technology, processes etcetera but the Australian Cyber Security Centre has recently published a beautiful document that I can actually send to you alongside with a whitepaper, I can send that to Maggie actually, which includes very specific and very thorough information that you can number one share with your cyber security auditors, share with your internal cyber security team if you have one and if you don't have one you can share it with your partners and third party providers that provide IT to you as well. Right, so that would show you what kind of threats are potentially, at the moment, what kind of threats are facing your industry right.

I got distracted because someone was trying to join. So welcome to the newcomers.

Step number two is to perform a compromise assessment but also perform a compromise assessment can mean multiple things. So number one, perform a compromise assessment then why's that important is because you want to know what exactly is happening in your environment after you have done your research. So you want to be sure that something is really happening and within that perform a compromise assessment you can choose to hire a company to come and do that for you, which I'll personally recommend, because the internal teams usually are very busy with tactical items and with protecting the environment. If they have to perform an assessment sometimes it might not be necessarily successful. So having a third party that does that for a job would be very very powerful for you to get the objectives you want to get. So you can also perform something called threat hunting and red teaming. You can also have a blue team, which will be the protection team, and the red team will be trying to constantly attack your systems and act as a malicious attacker where the blue team is trying to protect them to detect those threats and protect the systems. So the two teams together can be called purple team but I'm not going to bore you with too many details, you can find that information with any particular pen testing company that will help you out with that and *inaudible*. And this is extremely important *inaudible* to the fact that I know some of you are regulated and have to comply with PCI DSS for example. If that is your case, you probably have to do penetration testing every six months. So having red teaming and blue teaming exercises done can be

extremely beneficial. Another very important point that I want to raise here within the perform a compromise assessment part is that you can also look for something called dark market scanning and that can give you an idea of how much data is out there on your organisation within the dark market. And there's specific tools you can use to do that. I know for a fact we have done simple exercises like dark market scanning recently for a client of ours which is a bank and they found that they were, for example, fake Facebook accounts opened under their name. They have found a number of credit cards being sold on the dark market with obviously their brand and they had the possibility and ability to take that information off the dark market and to number one purchase it and delete it and number two understand a bit more, it's more like a forensic investigation understand who's doing that or their motives and was it driven by malicious actors trying to make profit or was it driven by competition because that can also be the case in some instances depending on the type of organisation and the type of business you are in. And then potentially and eventually, but most importantly, think about the threats you are hunting. Many organisations, especially when it comes to cyber hunting, you know I have my vulnerability assessment done I know my vulnerabilities but unless you are able to link your vulnerabilities with your threats that are facing your particular industry or your particular environment, you're not going to know the likelihood and hence you're not going to be able to evaluate the risks associated to your particular environment. So that's why threat hunting and threat understanding is so important.

Moving on, step number three on have I been hacked - plan. Plan, plan. And what that means is have an incident response plan because if you have not been hacked consider that you might get hacked very soon or if you have not been hacked consider that you might not know that you have been hacked. So be prepared. No matter what happens incident response planning will always be very important. For example, with the coronavirus that has just hit us, obviously it hit us six months ago so just, but still it changed the way we work, it changed everything about how we perceive threats, how we perceive incidents. And most of the organisations, not to mention from the 95 to 99% of the organisations didn't have incident response plans that included a pandemic, obviously because that was never on our radar. So incident response planning is extremely important. It will give you the ability to respond and as a consequence to uplift your resilience as we were talking about before.

So how to stop it. If I have been hacked, how do I stop it?

Number one cover the basics. Cover the basics means simply understand what are the hackers targeting within your environment and why would they be targeting it. Usually, in most instances, it's data. They're looking for data. They're looking for some sort of data because data is a currency. So understand your data, that's what cover the basics basically means. Once you have understood your data make sure that you classify it and I know it may sound like a very difficult thing to do but it is the thing for you to do in order for you to really understand how to protect yourself. Because unless you know the data, you're not going to know how to protect it unless you know where your data sits you're not going to know how much to invest to protect your assets right. So cover the basics is understand your assets, understand your data. But also

do asset discovery. Do you have shadow IT and if you do, how does it look like? What can I do to protect it right? So number one, cover the basics.

Number two. Take an attack based approach to security and I'm going to dive into that shortly, a little bit deeper. And I'm going to show you something very interesting which is the anatomy of cyber attack and how does it look like when a cyber attack happens and occurs. Like what usually happens, what are the steps. So I'm going to cover that in a minute but take an attack based approach to security. And to put it in practical terms what that means is that you are looking at your environment from the eyes of a hacker. From the eyes of someone who is trying to create damage or to steal data or to, you know, fulfill their malicious intentions so to speak.

And then number three, get strategic. This one is one of my favourites because it gives you the ability to strategise. And when we talk about strategy, getting strategic in cyber, it doesn't mean that you have to differ from organisational strategy, you actually your cyber strategy, cyber protection, cyber detection, cyber response and recovery strategy should be part of your overall organisation's strategy. That is why it's so important to be able to relate to different types of standards, for example, if you're working with government you would have the information security manual or ISM. You would have essential eights. If you're working with financial sector and you deal with debit card or credit card information you would have PCI DSS. But in general, no matter what you do, you would have to have some sort of mechanism to strategise about the future and what's going to be more effective and efficient for you. So one of those ways is to actually also have potentially a really well done risk assessment right. Because when you have a risk assessment, you would then be able to communicate based on those risks to your board and understand what exactly needs to be improved, what exactly needs to be tweaked, what exactly needs to be built from scratch etcetera etcetera. So get strategic.

Slide change

Guest - Gergana Winzer (Unisys): So let's get to the point of the anatomy of a cyber attack, which is what I promised to you before. And how does it all start? Here at the bottom you will see email web attack plus malware download. So this is when you would receive, or one of your employees would receive, a link with an attachment or it would receive something else and the moment the user opens or clicks or downloads that particular link or that particular attachment they unfortunately download either a virus or a malware. And when they download the malware the next thing that happens is that there is something that's called local machine takeover and that usually means that the attackers now are able to take control over your particular laptop or your particular machine or the user's laptop and machine. So once they have obtained that particular control what they are aiming to do is they are aiming for is something called privilege escalation. And privilege escalation means if I am, for example, working in HR and I don't have privileges to look in to accounting or to look in to sales they would look for the accounting or the sales or even the admin internal roles and the admin credentials to be able to escalate their privileges and be able to go sideways to go laterally within the environment and find out, obviously, different things and different types of data that they're trying to exfiltrate.

Indeed, the next part of the anatomy of a cyber attack is the data exfiltration. So once they have found the data, they're trying to copy that particular data to a location where they have the control.

So let's see how we're tracking with regards to time. So I don't want to bore you too much but raise your hands once again so I can see you are engaged. If you have received any kind of suspicious email or suspicious attachment in the last three months. Yes, that's right. Yeah same with me, I keep receiving those ones which is very interesting because it shows me that they can go through even the most sophisticated systems. Because at Unisys we have extremely sophisticated systems for security we are a defence grade security company right. So even in that case scenario we keep having those. But interestingly enough our CISO is a very progressive man so he keeps sending us those to check constantly how are we tracking and how many people actually jump into it and click on the wrong link so to speak. So it's a constant improvement once you know that this is how it works you have to put processes in place and techniques in place to make sure that your employees are not clicking on those emails. So they're aware not to open attachments and all that kind of stuff. So it is extremely important that it all comes down to the human element as well. That is why we have decided to call it the anatomy of a cyber attack.

Slide change

Guest - Gergana Winzer (Unisys): So there are different paths to resilience and as I mentioned before if you already have been implementing ISM, if you have already been implementing PCI DSS you already have some sort of a basic maturity or you have some sort of a baseline maturity level. Or you might be even further down the track and you might have managed security level if you are complying with PSF or our ISM etcetera.

So it depends where you are on your journey. If you have NIST, you might be on an adaptive level which I would be really really happy for you about because that's very difficult to achieve. But bottom line different ways to skin the cat so different paths to resilience. Like, similar to health, I would put the analogy back to health, there are different ways for you to be healthy. You may decide to do yoga, you may decide to do weight lifting, you may decide to do swimming but bottom line you'll be exercising to keep your immune system up and to keep strong. It is the same thing with cyber security. But one thing is where the experts come together and that has been in the last few years the buzzword called zero trust. I'm sure many of you have heard about it. Actually thumbs up if you have heard about zero trust before. Okay, I can see a few hands up, a few thumbs up brilliant. So zero trust is a way for you to achieve cyber resilience. Look at it from a pragmatic standpoint because many vendors out there may try to sell you something telling you that's going to give you zero trust. That's never the case. Zero trust, as does everything in cyber security, it's always technology, people and process. It's never just one technology that would do it all. However, zero trust also means that you are assuming that no system or no identity within your organisation can be trusted and as a

consequence you have to create things around those accesses to make sure that you can trust and then allow them access that they need. Or in other words have a business justification of why someone should be accessing something and working with that type of data.

So I have put some interesting concepts here for you to kind of bring it all together and give you that feel for what zero trust could look like.

So number one, know your network. Know and control your network because unless you know and control your network, you're not going to know how to actually prevent or how to protect yourself from cyber attacks. Actually prevention, let's put it that way does not exist. Where in the health world you practice prevention to prevent yourself from having diseases and from contracting any health issues with cyber that does not exist as a concept. You cannot prevent. So the only other option you have is to learn how to control. And in order for you to do that number one is always visibility. Visibility, visibility. Know your network. That is why I have put that point over there.

Number two would be encrypt the data in motion. So make sure that whatever data has been transmitted within your organisation, in and out of your organisation, between the different applications, between the users that data is actually encrypted in motion. Why's that important because we have all been using VPNs right except for us at Unisys we have our internal IP systems. But if you're using a VPN, what that means is that there is a potential for someone to attack that VPN and sniff the data out of there. But if that data is encrypted, they're not going to be able to do anything with it. So that's why encrypt the data in motion. Make sure that that data is encrypted and is rendered unusable by hackers.

Then irrefutable identity. Which is what I was talking to you about before. So why is identity so important is because whoever pretends to be somebody else, they can get data out of your environment. So by making the identity of the people who are accessing your network irrefutable, you would be able to mitigate those risks and to create that particular control over the identities that enter your environment. So you could authenticate with multi factor authentication MFA or you could authenticate with physical and behavioural biometrics. There's multiple ways to skin the cat. We could choose the one that is more relevant to you, to your environment, to your business because if you have a small business there's no point, then there's no point *inaudible.* But if you are dealing with critical assets, critical data, secret data, classified data then obviously having those controls would be extremely vital and important to you.

Then we go to cloak critical assets and that means is, cloaking is a concept that exists in the military world and we at Unisys have obviously adopted it because we work with defence quite a lot all over the world with Five Eyes. And cloaking means that you are able to cryptographically hide and render invisible the targets that are present in your network. So for example all your laptops or all your servers would be rendered invisible. And why's that important is because you cannot hack what you cannot see. So they cannot be seen right.

Then easy zero trust. Why do we say easy zero trust is because you need to know how to reduce your attack surface across all the different types of environments you might have because today we obviously have multi-cloud, we have at least one cloud, on premises infrastructure, all the different devices the BYOD etcetera etcetera. So we need to make sure that we reducing the attack surface and that can be done through cloaking the critical assets and obviously enabling the encryption of data in motion etcetera.

And then eventually enabling adaptive security. That's another buzzword that I particularly like, because what it does, it talks about how you can integrate what you already have to your different systems and create that ability to correlate and then be able to detect and respond meaningful. So, for example, if you're using one of our products for example Stealth and you're using a security information and event management system or in other words SIM, you would be able to correlate that data and be able to do something called dynamic isolation or isolate the targets that have been compromised. So let's say my computer has been compromised and there is malware on it because of the system Unisys has, they are able to isolate my laptop and do not allow me access to the critical data that I have access to otherwise.

Wonderful so I have been speaking for quite a long time, maybe Maggie you can tell me how long we have left because I am now open for questions.

Slide change - presentation ends

Presenter - Ian Gibson (ABSIA): Excellent, thank you. We do have a couple of questions that were sent in early. But before we do that, just wanted to comment on something you mentioned which is around VPNs. I'm not sure how many people realise but there was a review that was done about the end of last year that highlighted the fact that many of the, particularly the free VPNs, are in fact developed by Chinese companies. Now obviously I'm not paranoid but when people use VPN programs, they might want to look at who's actually provided them.

I thought that was a very interesting discussion around the threats and what happens when you get hacked. I suppose one of the questions that did spring to mind Gergana was if something like happens, you know, what's the first thing that an entity should do, like, as fast as possible.

Guest - Gergana Winzer (Unisys): That's a very good question Ian and there a number of different things. So, for example, if you have a regulatory body that is regulating you, clearly you have to be able to communicate to them. But the first thing as fast as possible would be to inform the board. Because obviously the board needs to know what the risks are. There are some liabilities and obligations to be met. So the board would be the first particular body that needs to be informed and then from there on, what needs to be done immediately is start an investigation. Isolate or stop or shut down the systems that are being compromised that you know of that are being compromised right. So these are the first few steps. And why's that important is because unless you have that internal accountability and responsibility you know to

bring it forward and to be able to make informed decisions, you're not going to know as a company what to do. And I know, actually, of executives who have lost their jobs because there was an incident and they did not communicate to the board straight away.

Presenter - Ian Gibson (ABSIA): As a Director, I'm glad to hear you say that Gergana.

Guest - Gergana Winzer (Unisys): I am sure.

Presenter - Ian Gibson (ABSIA): Now as many people on the call would know, ABSIA did a survey earlier this year where they found that 66% of respondents believed that attitudes towards cyber security had changed as a result of working from home. But I just wondered, given your experience, what are you seeing. Are you seeing something similar or are you seeing a different response?

Guest - Gergana Winzer (Unisys): Yeah, that's again a very good question. You know there has been different situations where we thought people are going to lose it completely because there have been a lot of attacks given the fact that people work from home. So we had, actually, an accounting firm calling us, because we have an investigation arm at Unisys right, so this accounting firm gave us a ring and said we had somebody calling one of our head accountants and telling them that they were from Telstra and told them to open their laptop and log in to his system so they had to do some maintenance because his internet, those people said to the accountant that the system was going to be hacked because they knew about it because they are monitoring the network. So that person opened the laptop and entered into the system and guess what, this was not a maintenance call. So he saw something weird was going on on the screen, he had no idea what was actually going on but bottom line they were getting hacked. And these are the kind of things we have to think about when we work from home. People will always be the weakest link. People will always make mistakes. So as cyber security professionals, we need to minimise the ability of people to make mistakes, while enabling them to do their job to their best ability even more. So if you want to put it that way, we are in a way enablers and these kinds of situations will keep happening. We also had issues with the health sector a lot. Like, for example, a few hospitals were hacked at the height of, you know, preparing for response to COVID in Australia New Zealand and that's obviously not going to stop the criminals right. So we have to be aware that those kinds of situations will occur. We have to be prepared for them, hence build cyber resilience not aim to stop necessarily or prevent attacks because as I said before, there's no way to prevent them, they will keep happening. But it's a question of rather build up resilience, build up muscle make sure that we have the ability to respond.

Presenter - Ian Gibson (ABSIA): In support of that, I saw a survey that came out of the US in March that I think, they said that the first month the number of vulnerabilities that have been reported had doubled and so I think everyone can see evidence regularly that that's occurring.

Guest - Gergana Winzer (Unisys): Yeah.

Presenter - Ian Gibson (ABSIA): Given that obviously Unisys is a large company, as you mentioned, gets involved in defence and other exercises. What are you seeing as being the key trends at the moment. Perhaps, you know, the ones that you are able to share as distinct from the ones you are not able to share.

Guest - Gergana Winzer (Unisys): Well one of the buzzwords that has been around, that's a really good question as well.

So first of all, I really wanted to address what you mentioned before about the vulnerabilities. Up until 2014 we had about 8,000 vulnerabilities known worldwide and you guys are in the software industry, obviously the biggest vulnerabilities come in to software right. Like they will always be in software. So what is very interesting to me is how from 2014 up until now we have tripled, quadrupled, like I don't even know quintipled [sic]. How do you say five times in English?

Presenter - Ian Gibson (ABSIA): Five times will do.

Guest - Gergana Winzer (Unisys): Five times. So we have seen a huge increase of vulnerabilities around the world and that has been pretty concerning because the more vulnerabilities we have the more there will be avenues to exploit those vulnerabilities. That is why I was talking about being able to connect the threats to the vulnerabilities to establish risk. Because if you don't do that, you'll just be trying to fulfil some sort of a patching mechanism and patch systems and all that kind of stuff. By the way one thing I didn't speak about is patching but patching is extremely important. Being able to have a meaningful patching practice within the organisation makes all the difference in the world right. So patching is extremely important.

And with regards to what you were asking me before, I have actually prepared something for today's participants. And what I have prepared is we are at Unisys, we are happy to offer for the first five companies that reach out to you, Maggie and to you Ian, we are happy to offer a one-on-one 30 minute consultation around cyber security risk and resilience and give them some pointers on how they can optimise what they already have. So we are happy to do that as a service to the community of the software industry because we consider ourselves as part of that community given that we are a system integrator and we bring all the different softwares together and make them work together in a meaningful way.

And to answer your question from before. What we have seen happening very much in the country is that desire to bring the controls high. That desire to increase the cyber security posture of the organisations. And I've been in the industry since 2012 in Australia and what I have discovered so far is that there's been a huge uptake in improving cyber security in general. When I look back in 2013, 2014 barely few people knew about PCI DSS. Barely few people were doing penetration testing on a daily basis. Now it is becoming commodity more and more and I'm very pleased to see that. So all the different agencies in Australia but also around the world based on the work we're doing are looking at improving that capability, that resilience.

Another important thing that they are developing as well alongside with ourselves is the ability to also implement something called offensive security. So not just defensive security, it's not just me defending myself but also me being able to be offensive. Like to be able to attack and to be able to respond in a way that also scare my adversaries. So offensive security is another important thing. That's why having or doing exercises like, you know, red teaming and blue teaming and purple teaming are so important.

Presenter - Ian Gibson (ABSIA): Yeah I'm not too sure how many people on the call would be familiar with this …

Guest - Gergana Winzer (Unisys): Let's do a poll. How many people on the webinar are familiar with offensive security, raise your thumbs up. Have you guys heard that before?

Presenter - Ian Gibson (ABSIA): Yeah.

Guest - Gergana Winzer (Unisys): Yeah I can see a few people. Great so I think I've given you a bit of details on that but happy to take many more questions.

Presenter - Ian Gibson (ABSIA): Yeah, yeah. I was just going to comment that it's interesting the recent cyber security announcement from the Federal Government allocated money. And it was interesting, a part of that allocation was specifically around the Australian Signals Directory developing an offensive capability.

Guest - Gergana Winzer (Unisys): Exactly.

Presenter - Ian Gibson (ABSIA): And it was a significant amount of money and obviously you know that's quite a shift in the thinking that's been going on in that area.

Guest - Gergana Winzer (Unisys): Correct.

Presenter - Ian Gibson (ABSIA): I had a couple more questions and maybe this one touches a little bit around budgets but there was recently, a survey came out with CISOs, chief information security officers for those sometimes we all get caught up in our acronyms, that they want to spend more money on cyber security. But then when they surveyed the business, the businesses were saying no actually looking to decrease their cyber security budgets. What are your thoughts on this, what are you seeing?

Guest - Gergana Winzer (Unisys): To be honest, I love this question, this is like the juice of the conversation. Because it is not just because of COVID they want to spend more money. Like traditionally, in our industries, the chief information security officers always had a little bit of an issue asking the board for money and that is not because they're not good at doing their work, they're absolutely amazing at doing their work. It was in the function of the fact that they did not know how to articulate the risks associated to cyber in financial terms to the board so the board

would actually know what they're actually paying for right. So that is one of the things I have discovered is that the moment a CISO or information security professional goes to the board and asks for money, if they know how to translate it in a language that resonates with the board, the board would not say no. Because obviously the board needs to protect their own obligations, they need to protect, you know, their own requirements so they would not say no just for the sake of saying no. They would rather say no if they don't understand what they have to spend money. Now, with COVID, that whole situation is shifting because everybody needs to save. It's not going to be just the CISOs that need to save, it's going to be the CIOs, it's going to be everybody, the COOs. They will need to save money for the business to be able to be resilient from a business perspective and also for the business to be profitable. So as a consequence, one way to skin the cat and one way to become a more effective CISO that asks for the right type of money, is to be able to communicate to the board but also be able to say I'm going to be a transformational CISO. I'm going to use all the resources that I have and I'm going to make sure that I understand what I have, how can I optimise it? So start thinking optimisation right. Start thinking how best can I use my resources? And actually I'm going to bring something from personal development to the conversation because I've been following Tony Robbins over the years and one thing that really stood out for me is when Tony Robbins says do not worry about the resources, worry about how resourceful you are. So resourcefulness comes up to be much better than having the actual resources right. So I invite the CISOs that I work with to actually become resourceful. Think about how they can do better.

But the other point that I wanted to tell you, for two of the participants on the call I'm actually offering one-on-one one hour session on how to ask for money to the board. And I'm going to that personally, maybe using one of my senior executive consultants to do that. But that's something I'm very, very happy to do because it's one of my passions to, you know, teach people on how to do that.

Presenter - Ian Gibson (ABSIA): Be careful what you say because I'm already getting private messages from people taking you up on your offer.

Guest - Gergana Winzer (Unisys): I'm happy to *inaudible.*

By the way, I saw a few messages in the chat.

Presenter - Ian Gibson (ABSIA): Yeah.

Guest - Gergana Winzer (Unisys): Are there any other questions …

Presenter - Ian Gibson (ABSIA): Ah no, they're mainly around copies of the presentation. Ooh there is a question here. Is there any recommendation on how to deal with things we usually do not as sensible as it is really like test environments, local documents and some less important things. We usually overlook servers and forget the small things.

Guest - Gergana Winzer (Unisys): Yeah. That's actually a really good point and unfortunately for many organisations that have not been traditionally focusing on security that is the case. Like you're not alone.

So first of all test environment is very important because in some instances, actually in many instances, I have seen people put real data in their test environment, which means that that data then becomes a target. So test environment is very important. And overlooking other servers, that would always depend upon whether or not your applications on those servers or the data on those servers or those servers themselves are connected to other critical systems within your organisation. Because if they are, then they are not not important, they are important. Because obviously they represent an access to those particular other critical systems that you have internally. So my recommendation would always be - do the basics right. Which is find out your data, classify your data and then think of how you're going to protect it. So as soon as you know what kind of data you have where, you know how to protect it. But also think about identity because, see, we have been thinking in our industry for a very long time about building walls, creating walls around the perimeter. Like this is my perimeter, these are my 10 systems, 20 systems, 10,000 systems, I'm going to build a wall around it and I'm going to build a bigger wall, bigger, larger wall. Now that has completely changed obviously over the last few years and now we have the identity, the person is the actual perimeter. So how am I going to protect that new perimeter, there are many ways to do it. One way can be obviously micro-segmentation, micro-segmenting based on identity and all that kind of funky stuff with the solutions that we offer but then potentially and eventually it will come down to how well you've done your background work. How well do you understand your data that you have? How well do you understand the connections and data flows within your organisation to then be able to meaningfully protect them. I don't know, have I answered the question?

Presenter - Ian Gibson (ABSIA): Yeah, no. I think so. And I think, in fact, with that question it brings us to a close. We have gone a little bit over time.

Guest - Gergana Winzer (Unisys): Oh sorry.

Presenter - Ian Gibson (ABSIA): No that's okay. It was good. Cause we had lots of questions. And of course it would be remiss to remind our members on the call that the SSAM network that ABSIA helped to develop jointly with the ATO. Is a part of one of the ways you can increase your resilience and so I would encourage everyone to sort of look closely at that if they haven't already.

I want to thank Gergana for what's been a really interesting presentation today. Obviously we can tell that from the number of questions that have come in. For those people that are interested in Gergana's generous offer, and we've already had several people respond that they want to take that up, I would encourage you to do so quickly before they run out. And I'd like to thank her today for her presentation. Thank everyone for participating and joining us today. Thanks for that.

Guest - Gergana Winzer (Unisys): Thank you for having me.

Convenor - Maggie Leese (ABSIA): Thank you everyone. We'll get in touch with everyone that has asked about the sessions and let you know what is happening there and get you in touch with Gergana. So I would like to thank you all for joining as well. And have a great rest of your days.