REPORT ON PROCEEDINGS BEFORE

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

CYBERSECURITY

CORRECTED

At Macquarie Room, Parliament House, Sydney, on Thursday 29 October 2020

The Committee met at 10:00.

PRESENT

The Hon. Tara Moriarty (Chair)

The Hon. Trevor Khan
The Hon. Taylor Martin
The Hon. Adam Searle
Mr David Shoebridge

PRESENT VIA VIDEOCONFERENCE

The Hon. Lou Amato

The CHAIR: Welcome to the first hearing of Portfolio Committee No. 1 for its inquiry into cybersecurity. Before I commence, I acknowledge the Gadigal people who are the traditional custodians of this land and I pay my respect to the Elders of the Eora nation, past, present and emerging, and extend that respect to First Nations people present. Today we will hear from industry groups including the Australian Information Security Association, AustCyber, (ISC)2, Active Cyber Defence Alliance, Vault Cloud and ISG Consulting Pty Ltd. We will also hear from Unions NSW and the Global Innovation Chair, Professor in cybersecurity at the University of Newcastle. Before we commence I will make some brief comments about the procedures for today's hearing. Today's hearing is being broadcast live via the Parliament's website. A transcript will be placed on the Committee's website when it becomes available. Parliament House is now open to the public.

All visitors, including witnesses, are reminded that they must have their temperature checked and register their attendance in the building via the Service NSW app. Please see the secretariat if you need assistance with this and please remember to maintain appropriate physical distancing at all times. All witnesses have a right to procedural fairness according to the procedural fairness resolution adopted by the House in 2018. I remind everyone here today that Committee hearings are not intended to provide a forum for people to make adverse reflections about others under the protection of parliamentary privilege. I therefore request that witnesses focus on the issues raised by the inquiry terms of reference and avoid naming individuals unnecessarily. There may be some questions that a witness could answer only if they had more time or with certain documents at hand. In those circumstances witnesses are advised that they can take a question on notice and provide an answer within 21 days.

VIJAY VARADHARAJAN, Global Innovation Chair, Professor Cybersecurity, University of New South Wales, affirmed and examined

The CHAIR: Professor, you are welcome to make an opening statement if you wish.

Professor VARADHARAJAN: I would like to thank the Committee and the Chair for this opportunity. Cybersecurity, as we know, is an important strategic and critical area for the New South Wales Government but also for Australian society at large. It is a key enabler for establishing trust in society. I am pleased that the Committee has chosen to do the inquiry and I hope the deliberations and the inquiry will lead to beneficial outcomes. In my opening statement I want to briefly set the overall cybersecurity context, the trends that we are currently faced with. Having been in cybersecurity for over 35 years internationally—in the UK, Europe, US, as well as in Australia for the last 20 years or so—at the outset cybersecurity is much more than technology. As I see it there are at least four pillars in cybersecurity. There is technology, the business or the organisation—whether it is government or industry—social aspects, as well as the legal aspects.

In the technology space we have seen dramatic developments in technology. In my view I think the technological change and innovation will be faster and more consequential in the next 20 years compared to what we have witnessed over the last 20 years. There are clearly some trends which we are seeing. The first one, obviously, we have been witnessing the growth in cloud services infrastructure in different sectors, whether it is healthcare, finance or any other sector. The other area is the plethora of devices that we are connecting to, the internet and mobile devices, which we refer to as the Internet of Things these days. The third area, which in my view is important, is the large scale data applications that we are using to make data driven decisions, and sometimes intelligent decisions, increasingly more so-called intelligent decisions, and that area is referred to as big data. The fourth area, in my view, which is critical, is bringing together cyber and physical systems.

In all these areas issues of security, privacy and trust are very significant. The other thing which we are doing is there has been an explosion of data and we are sharing data with the devices, amongst ourselves, and more importantly, devices are sharing data amongst themselves. In my view, perhaps the defining challenge of our time in the digital world is the truth, the veracity of the data, or the alternative facts, the fake news, because that underpins pretty much everything we do. It affects not only democracy, but also whether we use healthcare or financing, anything we do, this is a significant area. Data has many challenges, including the blurring of lines between what is private and what is public. In recent times, with all these technological changes and developments what is compounded is the effect of COVID and, in my view, the change in the geopolitical context that we have seen over the last few years and we will increasingly see in the years to come.

This brings us to a couple of topics particularly pertinent to this inquiry. The first is in this environment of the geopolitical changes as well as the technological developments, the first area is the one that you have in your terms of reference which is cyber incidents or data breaches or attacks. In this context my observation is that we have been witnessing a dramatic increase in what I call threat velocity. What I mean by threat velocity, there are at least four axis here. One is the vulnerabilities that we are seeing in systems, whether it is hardware or software, and how they are being exploited by adversaries, attackers, or people willing to do harm. This is happening because these systems are often complex. These are systems of systems and, yes, technology is improving but still when we talk about hundreds of millions of lines of code in the software area we are not able to write software which is secure or trustworthy at this stage. Most of the systems that we talk about these days, each system being hundreds of millions of lines of code and then they are connected together.

The second is the attackers themselves. We are seeing not just the hackers and the corporate espionage—that is where the money is and therefore it has always been there—but increasingly state actors. The difference is these actors have the ability to persist, persevere with significant resources. The third axis is we do not get too much time; the good guys do not get too much time to address these attacks. There is zero day attacks, there is no grace of time available to fix the problem beforehand. The fourth thing is that anybody—pretty much a novice because of the availability of sophisticated tools on the internet—is obviously able to do these attacks. If you put all these four things together, in my view, it creates an environment where we will witness these attacks, given the technological developments and the way we use the technology, and breaches will continue to happen.

We have to live with them. It is a question of being resilient. The urgency is, yes, we need the technologies. Yes, we need the framework. Yes, we need the software tools to detect, prevent, contain—that is sometimes overlooked—and recover from these attacks. There are four things when we talk about cybersecurity in this context. Apart from the technological thing, as I mentioned at the beginning, these pillars, we need to upskill people and we need to increase the awareness and ensure that the impact, the consequences of some of these actions can be understood by the community, but also have enough people to be able to solve these problems.

In this context it is worth mentioning that it is not a one-off thing. It is a journey, it is a process. We have to do this continuously. Also it is worth mentioning that there is no absolute security in the sense that these attacks will change, there are dynamic changes in attacks, so we have to be vigilant continuously. Having said that, equally important is that cybersecurity has a critical role to play in the economy, for growing jobs and for creating new opportunities. As I said, it is a key enabler for digital transformation for establishing interest.

Let me conclude by briefly identifying two points where the New South Wales Government has an opportunity in the context of growth of jobs and economy. I think both of them are outlined in my papers, so I will just be very brief. One thing to say is that I think the New South Wales Government has the opportunity to take leadership in the area of establishing, developing and maintaining minimum standards in Internet of Things [IoT] devices. Why I am picking this out specifically is because out of all the different technologies IoT technology is going to be an element of the overall ecosystem where everyone in society—different companies, different users—will be involved in either using it or developing it and so on, so in fact there is an opportunity for the Government to use the procurement technique or procurement vehicle to ensure that the ecosystem of IoT has certain minimum security standards, so it can be influential in making this happen. Once it happens in the market, at the commodity level, then it has the added benefit of ensuring the overall security of the ecosystem. That is number one.

Number two is I think somewhat related, but given that small- and medium-sized enterprises [SMEs] are often the backbone of countries like Australia or the United Kingdom, or even New Zealand and other countries, it is critically important I believe for the New South Wales Government to enhance the cybersecurity capability of these, because SMEs often play a role in the manufacturing of IoT devices as well, so there is a connection there. Whatever we do to enhance the cybersecurity capability of SMEs has an amplified effect on the economy. Coming from Newcastle where I have been for the last three years—I have been working with the Hunter region—I have seen a lot of SMEs and when I talk about enhancing capability what I mean is giving them strategic and thought leadership advice, helping them with their current products and future products, helping them with engagement of Government agencies because of compliance, as well as specialised training, and especially in regional areas there is an opportunity for the New South Wales Government. With that, let me finish my opening statement and I will be happy to answer any questions the Committee members may have to the best of my ability. Thank you.

The CHAIR: Can you talk us through, with a bit more information, what threats are facing the New South Wales Government in particular but also the people of New South Wales in terms of our information? Is it State threats from other countries, is it criminals that are trying to steal our personal information? What are the biggest threats that we are facing now?

Professor VARADHARAJAN: Thank you for that question. Threats in general in society happen. If one looks at past records—and when I say "records" I mean surveys and other things we have done—most of the threats are often in the area of where the money is, so it is to do with criminal activities going after money. That is the primary area. If you look at the curve, at one end of the spectrum you have individual hackers who do things, but the chunk of it is criminals going after money. Increasingly, what I call the state actors do not necessarily at this stage have—they have very targeted interests. If you look at individuals getting attacked, it is unlikely those will be the state actors. Individuals and SMEs are primarily in the area driven by money.

The problem with the attacks is the following: People will always go for low-hanging fruits first, so if there are vulnerabilities in society, and I particularly take the IoT market where there is a vulnerability, it is opportunistic for attackers. In COVID times we would see phishing, we would see business email compromise, we would see the taking of credentials and identity theft. These are quite common, and the return on investment is good, so always the attackers look for low-hanging fruits. With respect to state actors, it is a long-term gain, and I think if you look at the Australian Federal Government strategy, which was released in August 2020, I think rightly it has emphasised critical infrastructure. The notion of what is critical infrastructure used to be telecommunication networks and financial services and so on, but now cloud data centres are critical infrastructure and health care is critical infrastructure as we talk about taking people's personal details.

The answer to your question is that the attacks are, firstly, quite widespread. Secondly, always the attacker—he or she or the group—thinks of the return on investment. Money is a primary driver, so where there are opportunities where I can get quick return, that is clearly the case. Now with IoT devices, with mobile devices, with the ubiquity of network connectivity, society as a whole—and it is a fundamental problem we have—is aware of it. Compared to 10 years ago there is a lot of awareness, in my view, but we still do not sometimes take things seriously and therefore our systems become vulnerable, our behaviour becomes vulnerable and then can be exploited. I think that is where the majority is. Having said that, these technologies, especially nowadays given the geopolitical situation, and we have to be very careful because—I mean take the supply chain security, one of the issues that we have had with respect to COVID. It equally applies in the cybersecurity space.

I am saying a few things, but I am not directly answering your question because all the surveys would probably say that the majority of the area is where the financial crime is, and that is not just the financial industry but where I can get a financial return. That is where the majority of this is, whether I am selling data, healthcare data, to somebody or whether I am duping you to get your password credentials and therefore I can log into your financial services, or whether I can use some of your mobile devices to get some personal details and then perhaps use those to my advantage.

The advantage is primarily financially driven. That is where I see the major thing. But the technologies, the vulnerability of technologies, are open to be exploited by actors who have the ability, and therefore clearly there are actors who have the ability, you know, the geopolitical situation, and therefore we have to ensure that we are serious about cybersecurity throughout the life cycle. It is not a one-off thing. We say with COVID that until a vaccine comes we will wash our hands, use sanitiser, and then we may be able to relax. The problem with cybersecurity is you have to be vigilant continuously, all the time.

The CHAIR: In your experience, do you think the New South Wales Government is as vigilant as it should be? Is the Government taking this as seriously as it should be? Are there enough resources being put into this? There have been a number of well-known breaches over the last 12 months—Service NSW, Transport for NSW.

Professor VARADHARAJAN: Yes.

The CHAIR: Where are the gaps in the New South Wales Government cybersecurity?

Professor VARADHARAJAN: I am not privy to all of the information of the New South Wales Government, but from what I have seen—and I have read the 2018 Auditor-General's report—certainly certain improvements can be made. I know that subsequent to 2018 there have been major developments, they have established a governance structure, they have established some mechanisms for responses and they have established a way of coordinating information from different agencies. I know they have done all these things and I heard in June 2020 they announced $240 million or so over the next four years.

I would like to answer the question in the following way: I think those are all good. Establishing government structures is critical, in my view, and establishing what each agency should do to detect, prevent and respond effectively is important. Establishing the collaboration or the trusted information sharing between agencies is critical. Establishing an accountability process is the right thing to do. The question you asked is, have they done it sufficiently? I am not able to answer that because I do not have the visibility into whether they are working or how well they are working. I have not seen any reports or feedback on these stats. That is number one why I am unable to answer that question. The second thing is that, in my view, as a I said, it is a continuous process. How do we know whether it is working or not? That is the first question that was asked. We only know whether it is working or not if we are seeing that the data breaches have gone down or we should have a metric to do that.

We have the policy, we have the framework—I do not know the right internal metrics being established. But from the external point of view we see the data breaches happening from what we read in the public media and elsewhere. So it is critically important to have a metric and to measure the metric, to report on it and continuously drive to improve the metric. That process has to be there. The answer to your question is: In some sense, once you have established a policy, have a board that continues to look at the strategy and have established a metric, then you have all those mechanisms put in place to progressively check that and ensure that those types of attacks are not happening.

They will continue to happen. I will give you an example. We walk the streets and cross the road knowing that cars will be there and we may be susceptible to being hit by a car. Similarly, there will be attacks and we have to survive with the attacks. That is why resilience is important. In the COVID situation we are driving the numbers, that is the metric we have. In security, the metric is very difficult, though. People have a profile of things but that is not in itself sufficient. We have to continuously ensure that we are able to recover and contain the attacks.

The CHAIR: Is it currently not mandatory for government agencies to notify of data breaches?

Professor VARADHARAJAN: Correct.

The CHAIR: It is not mandatory for them to notify people if their data has been breached. Do you think that should be happening?

Professor VARADHARAJAN: Absolutely. I know that at the Federal level we have a mandatory notification of data breaches and I know that that does not apply to New South Wales public agencies. I think we should. There should be consistency between the national and State ones. Often, if you only get to notify, at least the organisations will put in place some mechanisms to detect those attacks to improve the organisation. It will help the individuals, groups or organisations that are affected or harmed to take some action and the agency could also help. What about what the Office of the Information Commissioner at the Federal level is doing with respect to assisting the individuals and with respect to harm? All those things would be useful but, most importantly, I think it will help to improve the consciousness, awareness and the ability or confidence of organisations to detect and respond to those breaches. I think those laws should be applicable to New South Wales.

The CHAIR: So that the breaches cannot be kept a secret?

Professor VARADHARAJAN: Yes. There are different types of breaches. But this is where, if we look at the legal framework, it will say that it depends upon the amount of harm that is being done and that is a subjective thing. But, yes, the breaches should not be kept secret if they are affecting the livelihoods of people and can be improved by making them public. That is the litmus test, there. Also, it will increase the responsibility of the organisations to put procedures and mechanisms in place to detect the breaches and to help externally. I think both sides of the coin have benefit. But when one looks at the law there are sometimes cases where you do not want to publicise those harms; sometimes there are cases where we do not know how to communicate the harm to the intended person and it has to be taken with care.

Mr DAVID SHOEBRIDGE: Professor, you talk about the Internet of Things as being the most obvious risk going forward. Would that be a fair description?

Professor VARADHARAJAN: Yes, it is one of the four things I outlined. I picked up Internet of Things for the New South Wales Government because it is something that is low-hanging fruit and they should be involved in that.

Mr DAVID SHOEBRIDGE: Can you give a practical description of what you see as a viable threat from this increasing interconnectivity of ordinary devices?

Professor VARADHARAJAN: Let us imagine that I have a device that is monitoring traffic lights. Suddenly, there is an intersection where I make a couple of those traffic lights green at the same time. A very simple example. I could create minor traffic chaos or I could create different types of traffic chaos at different places. That is one example. The other example is in the industry or control system I might have some SCADA devices, or some devices telling me readings of temperatures or different types of things that I am monitoring. If I were to attack one of those devices and it gives me the wrong reading, I might do something totally different with respect to my power plant, for example.

Mr DAVID SHOEBRIDGE: Is the increased vulnerability through the Internet of Things that those devices are of themselves just connecting to the broader internet, rather than having a narrow connection inside an industrial or government process?

Professor VARADHARAJAN: Correct. The first thing is that every device has at least two things. Even in a trivial device there is a little bit of software running and then there is the connectivity. When those two things are attacked they could be vulnerable. The connectivity is, because, as you rightly said, previously they were only connected inside a local area, inside my organisation, now they are connected externally—maybe internet, maybe other networks, not necessarily the internet. That opens up the ability through the connection for an attacker to get to that device. That is number one.

Number two is that the problem with SCADA and those types of devices in the industrial sector. Many of them have been there for 20 or 30 years and they do not have any security functionality at all, but we are now exposing them to connectivity. Even if you try to update them—and what does update mean? You have to download some software into it. Often those devices have a very small amount of software. In principle, they can be written properly but, as soon as you introduce software that updates, there is a potential for vulnerable software to get into it. So it can give you wrong data once a day or twice a day. It can do all sorts of things. So the two things are connectivity and potentially the little software or something that resides in them.

Mr DAVID SHOEBRIDGE: When you say the State Government could set standards, are you talking about basic, minimum security standards that cover connectivity in particular?

Professor VARADHARAJAN: Yes. What I am saying is that there is an opportunity. For instance, at the personal level, there are a lot of reports— report into what should be in the IoT—in the United States, Nesta. We also have a lot of reports in our IoT space in Australia. The key thing is this, which I think you identified—one is the basic, minimum functionality I expect in different sectors. For medical devices, I expect that functionality to be there. The second thing I expect is that functionality to be—the claim that manufacturers are making—somewhat vetted or validated. I could use the word certified. At least somebody else has to look at it to say that the claim makes sense. One of the problems in many of those devices is that manufacturers make claims but we have no way—we have to believe those claims. So when I say standard I mean two things. One is some minimum functions, as you said, but it has to be sector dependent.

The second thing is some methodology process for validating that. Yes, there are many things that are not but I think it is important. In New South Wales the way to do it is not to develop a new standard. It is someone saying, "When I am procuring medical devices, I need this. When I procure devices for my energy sector, I need that." Let us do that. It will incentivise manufacturers to develop the products with those functionalities. That is the objective rather than setting up a standard a check list, in my view.

Mr DAVID SHOEBRIDGE: Are there Australian standards that are the starting point? We have other submissions talking about standards for training, I think ISO 17024 from 2012 and other standards about information, security and management, accreditation and they talk about ISO 27000:2018.

Professor VARADHARAJAN: Yes.

Mr DAVID SHOEBRIDGE: Does it with a standard? Is that how it works?

Professor VARADHARAJAN: Yes, I have been in standards for about 30 years. ISO 27001, it came from BSI 7799 and that gives you a checklist. That gives us a process but that is not, when you write standards, we write all this at a fairly high level and that does not necessarily apply to IoT. Answer to your question, right?

Mr DAVID SHOEBRIDGE: Yes.

Professor VARADHARAJAN: Yes, it can apply to IoT but it was not intended for that. One way of doing it, let us take a profile of that. Let us use that as a basis and write something for IoT devices out of a medical sector. Let us do that. That would be more helpful in my view. You referred to ISM. Yes, ISM has been the information security manual and that has been there for many years. There is also the National Institute of Standards and Technology [NIST] to cyber security.

Mr DAVID SHOEBRIDGE: Just translating all of this, does that mean that because the New South Wales Government is literally the biggest procurer of services and goods in the country, if it stated, "This is our standard for medical devices in New South Wales", maybe put by reference to these standards, but then set out a clear standard for medical devices and then made that generally available to private health and others that would then set a minimum standard?

Professor VARADHARAJAN: Yes, absolutely.

Mr DAVID SHOEBRIDGE: Then that might be what set the standard nationally.

Professor VARADHARAJAN: Correct. That is exactly what I am thinking.

Mr DAVID SHOEBRIDGE: And the same in the energy sector?

Professor VARADHARAJAN: Same with energy, and we can pick up the sectors that are relevant or prioritised strategically important for New South Wales. Let us do it for a couple of sectors, right. Let us build this secure system because somebody has to start. We cannot be like this, in my view. Yes, initially maybe very minimum, initially there will be deficiencies but we will learn. It is a living document, as you say, and the vendors and manufacturers will have a—that is how we develop all these standards, right, the de-facto standards? But there will always be international standards, yes, that is true. They have a role to play and they are important. Look, I am a strong supporter of standards but here is the thing that a standard is a double-edged sword, right?

Mr DAVID SHOEBRIDGE: They are something to shoot for if you want to break it—

Professor VARADHARAJAN: Not just that. They freeze the technology at a given point in time. In order for 10 people to agree on a standard I have to freeze that because it takes time for you to agree on the same thing. But while we are agreeing things are moving on, people are developing. So we have to freeze the technology to arrive at a standard, right? Therefore that is a double-edged sword, right? Then as you say, once I freeze the technology it focusses the mind, attacks happen but the standard remains the same. Right? But that is why the standards will be never—we do this thing but then we write profiles; instantiation of the standards. And this gives you another problem because there are a lot of vendors who will claim conformance or compliance to standards but they are not at all interoperable.

I have a product from vendor one and a product coming from vendor two. They are conforming to the same standard but they do not inter-operate because the reason is they do profiles and they interpret. Standards gives you multiple options. They choose the options in a certain way according to their business strategy and what their company is interested in and they end up with a standard. Standards, yes, it is important but it does freeze the technology. It focuses the mind and it may not necessarily mean they are inter-operable. Having said all that, standards are important for us to move forward.

Mr DAVID SHOEBRIDGE: Health care seems an obvious space. If you think about the increasing complexity of health care, the number of different devices that are used, say, in an intensive care unit, ensuring that, first, they communicate over time and, second, they are not vulnerable to an external threat, that seems like an obvious starting point.

Professor VARADHARAJAN: Yes. Health care is a fantastic industry to start and not only in your hospitals like what you are talking about, what we describe is a bit of a skunk work in the last couple of years, but increasingly what we are doing is we are embedding devices in the human body. The first thing is we do not have a single registry. Clinicians want to know in which patients I have put these devices? I just want to know and I want to learn neurological symptoms. But at this stage there are very few—I think I was told this was a bit of work in the health care, only for hip surgery. That is a national registry which was done about 10 years ago. There are a bunch of registries for other devices, especially in the Victorian sector, but really that is very basic low-hanging fruit. Which devices have I put in which patients? When did I put them there? What am I reading from them? Is the data right? Yes, in substance, within the hospital—you were talking about intensive care—we can restrict these devices talking within that environment. We do not need to open them up and all this stuff. So it depends.

The first thing in security is you have to look at the environment, assess the threat and then design the solution. But what is happening with the hospitals now is we have telemedicine and we are going to continuously, so it more connectivity and patient data. Five years ago one of the pieces of work I was doing was patient health records. At the time it was called PCEHR system—patient centric electronic health record, nowadays we call it this new health record. I have written several pieces on that. I have developed a technology. I talked to the Minister for Health at the time, to the department in the Federal area, how we can improve that. In the hospital there will be database, health records, hospital information systems. Some of them are open. Now increasingly we are using more connectivity into that. And then there is the devices bit. Each one of them will have slightly different requirements and standards but at least I think in the IoT case the devices is the one I was referring to but each one of them important, yes.

The Hon. ADAM SEARLE: Professor, we do not have much time. I will ask some questions and if we do not have time for you to answer them, could you answer them briefly and then maybe if you want to give us something further on notice, that is fine.

Professor VARADHARAJAN: Sure.

The Hon. ADAM SEARLE: Some of the submissions the Committee has received have talked about the need of the data sovereignty—that is, to make sure that the data is kept in Australian territory rather than on overseas clouds or servers. There are mixed views about the desirability of that. The balance of submissions seems to say that is the best way to enhance personal data security, national data security as well as creating local jobs and opportunities. What is your view about the desirability of data sovereignty?

Professor VARADHARAJAN: I have some experience in this on both sides of the fence, put it that way.

The Hon. ADAM SEARLE: On balance, what is your view?

Professor VARADHARAJAN: My view will be to say for certain types of data, which are critical and sensitive, I would suggest the sovereignty data centre. The data should reside within Australian boundaries. That is the over-arching principle. I can implement that using a variety of mechanisms. In other words, I am not saying anything about: Does that automatically imply certain providers will be excluded? That is not the objective. The principle is it should reside and we can implement that. We can ensure that happens even with different providers.

The Hon. ADAM SEARLE: In your submission you say that the security measures that the ASD refers to as Essential Eight is a good starting point for addressing security risks. What is Essential Eight? Does the New South Wales Government implement it?

Professor VARADHARAJAN: Yes, I think the New South Wales Government definitely implements it. The agencies within the New South Wales Government implement it. Previously, about a decade or so ago, ASD was involved at the time with the DSD, the top 35 listed, taken from the top 35. What is the Eight? Essential Eight will say something like, I think I referred to it in the paper, but patching is one. You should patch all your systems. These are all guidelines what you should do. It will say white listing applications so that means if I want to use Adobe, for instance, or if I want to use—I should not mention the name of companies—an application it should be listed as a good application, white-listed application, so that is another one. Ensuring that it at least privileged is a fundamental thing in security. It is a need to know in the world of defence.

If you need to know that information, you have the privilege. So we ensure that every process, program, application and system in your IT infrastructure has only the minimum amount of privilege for that application to do its job and no more. So these are the types of things—patching and then there is something about macros. There are eight of them like this, but I do not remember exactly which eight. Initially there was a list of 35. I remember those days where I used to say that if you implement the top four or five in the Defence Signals Directorate [DSD] 35, you will probably counteract about 70 per cent of the attacks, but there are always attacks that you will not defeat. So that is how this eight essentially got developed. I can talk about this, but I had better stop in this case.

Mr DAVID SHOEBRIDGE: ASD is the Australian Signals Directorate, and DSD is the former Defence Signals Directorate?

Professor VARADHARAJAN: Correct. It used to be the Defence Signals Directorate, but nowadays it is ASD.

The Hon. ADAM SEARLE: We have an outfit called Cyber Security NSW that is part of the Department of Customer Service, but it does not seem to have complete responsibility for cybersecurity across the whole of the State Government. It seems to be the responsibility of each agency, so no-one has overall jurisdiction. In answer to budget estimates questions last year from the Secretary of the Department of Premier and Cabinet when there was a major data breach, his evidence was that he did not do anything about it because he did not see it as his role. He thought that it was someone else's role. Is there the need for a strong single cybersecurity agency for the New South Wales Government to better safeguard the public arm?

Professor VARADHARAJAN: The answer is yes. There are two bits to that answer, and then I will add some peripheral things about what I have been involved in. Every large agency should have a cybersecurity unit which is responsible for its policies, the mechanisms and its Chartered Institute of Procurement & Supply reporting, and all that stuff. There should be a way to coordinate. Each of the heads of these agencies should belong to a forum, group or board where they can periodically report and come together, because there must be a way for these agencies to share information. Yes, there must be an agency which should be accountable overall to the New South Wales Government. That is how I will structure it. I presume that something like that was raised in the New South Wales Auditor-General report in 2018, and I presume that the New South Wales Government has established the chief security officer at the global level. They have done some of these structures, but it is not visible to me.

The Hon. ADAM SEARLE: You make the point that the current state of preparedness is not visible to you, so you do not know what the State Government has done to respond to the Auditor-General's report of 2018. There is no reporting about that. Should the State Government not be giving us some comfort that it has addressed all of those security concerns that have been identified?

Professor VARADHARAJAN: It should be, but how public that is is another question. But definitely my answer is yes.

The Hon. ADAM SEARLE: Just on that point, the Auditor-General's report is public.

Professor VARADHARAJAN: Correct, and therefore the response should be public.

The Hon. ADAM SEARLE: Should the response from the State Government also be public?

Professor VARADHARAJAN: Absolutely. It is important, and this is based on my past experience, that at both a large corporation and government level you establish a strategic advisory board. All of the things that I referred to—each agency has both operational responsibility and management responsibility, but one of the key things in cybersecurity in my view is to have thought leadership. They can tell some of these agencies what they might have overlooked because they focus on the day-to-day side of things. I think that is very important, so that was the point that I raised there. In my experience, that has worked very well.

The Hon. ADAM SEARLE: Do you endorse the findings by the Auditor-General and the direction the Auditor-General suggests the Government should take?

Professor VARADHARAJAN: Yes. It was a big report. From what I can remember, I think that the Auditor-General clearly mentioned the need for such structure and a whole-of-government cybersecurity policy, or something like that, and your previous question referred to that. The other thing I remember is there were some agencies where the mechanism, strategy and framework were not up to scratch.

Mr DAVID SHOEBRIDGE: The Auditor-General's polite language was "have a low capability to detect and respond to incidents in a timely manner".

Professor VARADHARAJAN: If the Auditor-General has done that, I presume that is the right thing. I accept what she is saying. You asked a previous question about whether the response from the Auditor-General should be made public, and the answer is yes, given that the report was public. How this is being done is not necessary to be made public. We can have a board or somebody who can regulate it. They do need to vet these things to ensure what is being done is at the right level. So you need some sort of a sanity check in my view. Security is one of the areas where you need a continuous sanity check, because things move reasonably fast.

The Hon. ADAM SEARLE: I am happy for you to take my last question on notice and come back to us. What will the Hunter Cyber Hub be when it is fully constructed and operational?

Professor VARADHARAJAN: In a previous life I was the Microsoft Chair Professor at Macquarie University and we established a hub with Optus. I am passionate about enhancing the capabilities of small- and medium-sized enterprises, and I am passionate about the fact that in regional places there are fantastic companies and there are opportunities there.

The Hon. ADAM SEARLE: Sure, but what will the hub be?

Professor VARADHARAJAN: It will help management of the small and medium-sized enterprises with respect to best practice. That is example one. It will look at the staffing of that and provide specialised training. It will work with the SMEs to engage in compliance with ISO 27001 or Essential Eight. But most importantly it will look at the current products they have and potentially help them to identify the next version of their product, and develop R and D as well. We all know that SMEs are cash poor and time poor and they do not have the expertise to do that. That is what the hub will do, in my view, and we need the New South Wales Government to encourage such hubs in regional places.

The CHAIR: Thank you, Professor. Thank you so much for attending today; we appreciate your time. It was really useful.

Professor VARADHARAJAN: I thank the Committee and I thank the Chair.

(The witness withdrew.)

TONY VIZZA, Board Member, Australian Information Security Association, sworn and examined

STEPHEN KNIGHTS, Director, Australian Information Security Association, sworn and examined

The CHAIR: Would one of you like to make an opening statement?

Mr VIZZA: Madam Chair and members of the Committee, thank you for the opportunity to provide input into the Legislative Council's inquiry into cybersecurity today. My name is Tony Vizza and I represent the Australian Information Security Association [AISA]. AISA is the peak body for information security, cybersecurity and privacy in Australia today. It consists of over 7,000 cybersecurity professionals as well as members in affiliated sectors such as risk management, cyber law and information technology. AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and New South Wales and advancing the cybersecurity and safety of the Australian public, businesses and governments in Australia.

AISA's vision is of a world where all people, businesses and governments are educated about the risks and dangers of cyber attack and cyber theft to enable them to take all reasonable precautions to protect themselves. As an independent not-for-profit association AISA was created to provide leadership for the development, promotion and improvement of our profession. Joining me here today is Mr Stephen Knights, a fellow director of the board of AISA. Students of history will be aware that societies around the world have seen different threats and risks at one time or another. Today's world is heavily reliant on information technology, connected systems and the internet that it throws up its own set of risks and challenges. Cybersecurity represents the modern embodiment of many of these risks and challenges.

In July of this year Prime Minister Scott Morrison told the Australian people that Australian governments and businesses were under sustained cyber attack. Federal agencies singled out the State of New South Wales as a specific target for cyber attackers following a number of high-profile breaches that occurred here, most notoriously the breach that occurred at Service NSW in April of this year. The Australian Cyber Security Centre recorded a huge spike in incidents nationally at approximately the same time, which of course coincided with the advent of COVID-19 and the related lockdowns. That saw people who were understandably preoccupied and anxious with the global pandemic make some poor decisions that saw them succumb to a wave of phishing campaigns, phone-based campaigns and other electronic fraud.

Cybersecurity and IT-related risks now make up two of the top 10 global risks both by likelihood and impact according to the World Economic Forum. In light of this, the question remains where to from here. AISA has of course provided a very detailed submission addressing many of the items listed under the terms of reference for this inquiry and has provided detailed recommendations for how the State of New South Wales can strengthen its cybersecurity posture. Today Mr Knights and I will seek to provide any additional insight, opinions or views to any questions that you may have. We base this on our own professional experience as well as the collective experience of over 7,000 members that AISA represents. It is our hope at AISA, as well as the personal hope of both Mr Knights and myself, that the recommendations made via the written submission and by our testimony here today will result in a safer and more secure New South Wales. Thank you.

The Hon. TAYLOR MARTIN: We are at the start of this inquiry process. I would not mind asking if we could just start at the very beginning and give other members who might not be part of this inquiry and people reading the transcripts in the future an idea of why this subject is so important. Effectively, what are the risks if there is a breach? Obviously there will be different levels of breaches. Could you give us an overview of what those different levels of breaches might be? What are the real-world consequences of having a lack of cybersecurity?

Mr VIZZA: The fundamental aspect of cybersecurity really comes down to the fact that we are sitting in a room right now where we have IT systems. I can see a videoconferencing unit. We are all working on computers. We all have phones in our pockets. We are surrounded by technology. The reality of it is that this is a critical issue for all people in Australia and in New South Wales. It is something that we all need to deal with and accept as a problem. We often talk about the fact that most people do not realise how much technology actually exists in their own homes. Our TVs are connected. We all have wi-fi at home and we all have many different bits of technology, all of which connect to the internet. As we heard the earlier speaker describe some of the issues related to IoT security, there are a number of different aspects of cyber security that need to be looked at. I think the biggest challenge is really in accepting that it is a problem to begin with. If we can do that, then we can start to deal with some of the problems that are inherent in this.

Mr KNIGHTS: You talked about the actual vulnerabilities and the kind of threats that we are under. The reality is that it is a people problem more than it is a technology problem. A lot of the concepts that we are talking about when we talk about standards, the process and things like that, what we need to understand is that the lack of training and awareness is the greatest issue. New South Wales Government as a leader in that space has an opportunity to come up with standards and recommended training programs that will help us close the gap. When I talk about the issue, there is what I call a top-down and a bottom-up meeting of the two divides. New South Wales Government has an opportunity to be a leader and set these standards and programs in place. We can raise the bottom up where we have people inside the New South Wales Government with adequate training and awareness, but also in the broader community. Unfortunately, with the current climate, COVID-19 has sort of taken the tide out and shown the rocks of what is going on in society. Unfortunately, when people are vulnerable and their mental states are fragile, they are more likely to fall prey.

Australia, being fairly affluent compared to other nations, is targeted because of this. One of the reasons why we are targeted is because we pay. When we are compromised, we open up our wallets and we give out money. We pay. That is a real challenge. That is broader society. When we look at what those vulnerabilities are doing to business, they are commercialising things. They are taking valuable data and they are actually able to sell it as a dataset in the black market of the dark web. There is proven commercial gain for these people. I am really just identifying that there are very sophisticated criminals. They only have to get it right once and we have to try to get it right all the time. The previous speaker talked about standards and that is where that comes in. At least we raise the bar to a starting point where we—I am talking specifically about the Internet of Things. We are making the same mistakes over and over by not having a minimum standard. Where speed-to-market is more important than security, we should at least set some standards where these mistakes are not being repeated.

Mr DAVID SHOEBRIDGE: Do you accept Professor Varadharajan's description of how the New South Wales Government could and should set standards for different sectors?

Mr KNIGHTS: I thought that was a pretty good insight. I had not considered doing specific sectors. I think there is a broader set of standards that probably is a minimum for the wider Internet of Things, but specifically higher standards for certain sectors seems like a very strong merit.

Mr VIZZA: I will just add that the Federal Government has indicated this in the critical infrastructure space. Under the Cyber Security Strategy 2020 at a Federal level, they are running a whole bunch of different workshops right now to come up with a set of standards for critical infrastructure—not only critical infrastructure but defining what critical infrastructure actually looks like. If you ask different people, they will have different opinions of what that actually is.

Mr DAVID SHOEBRIDGE: If you asked my daughters, they would say our wi-fi at home is critical infrastructure.

Mr VIZZA: Correct.

The CHAIR: You have talked about the opportunity for the New South Wales Government to show some leadership in this. Do you think that they are? Is the Government doing enough to protect our information and the information that is contained within agencies?

Mr VIZZA: I think that from an intent perspective, the intent is right. There is definitely the understanding that it is an issue. I think that the Government is also in the process of trying to execute that, mindful of course that this is a moving target. Sometimes there is that delay in trying to deal with the new threats that come out. The way that government operates, of course, there is a time delay between the threat emerging and then actually dealing with it. I think that the intent is there. I think there is more that could be done from an execution perspective and I think the Auditor General report makes it pretty clear in that respect and I would agree with the findings in that report. I think absolutely there is more that can be done. I think we are on the right track at this point in time. There is more refinement that needs to go into it.

The CHAIR: Would you include mandatory reporting in that? In your submission you detailed a number of incidents, many thousands of incidents that have been reported of cybercrime to police and other agencies, but if it is not mandatory for the government to even notify people how do we know if these are the only things that have happened?

Mr VIZZA: I would absolutely support mandatory reporting at a State level and at a local government level, which I know is not required under the Federal mandatory breach notification laws. If the State Government were to implement an arrangement similar to the European Union General Data Protection Regulation [GDPR], I think that would be highly beneficial in terms of that breach reporting as well as ensuring these cyber security and privacy-related concerns for a lot of people in New South Wales would be very much met by incorporating a GDPR standard here in New South Wales.

The Hon. ADAM SEARLE: What about data sovereignty? A number of the submissions we have received have said, look, at least certain types of data should be housed in Australian territory. That does not exclude overseas companies from providing those services but saying to maximise data security, national security and maximise local employment it is best to keep this data onshore. What do you think about that?

Mr KNIGHTS: I might give a practical example so you can understand how data sovereignty may be a very practical protection. One of the concepts of what we can do across the internet is we can actually isolate traffic from regions, and we can actually turn it off from geotraffic awareness. If there was a particular region that was doing increased particularly alarming traffic at a higher level we can actually block that and disable the traffic. Data sovereignty gives us great insight from a global perspective of where the traffic is coming from and what we can actually do with that traffic and when it is locally controlled we have controls over those measures. That is why that practicality of actually being able to control where traffic is coming from, what the traffic is doing and how we actually control and allow that traffic. One good example of what we can do is local traffic may not be under the same rigour as it is challenged as it would be from an international footprint. Data sovereignty actually can create some practical measures on a global footprint of how we look at the way the traffic is coming in to access our systems.

Mr VIZZA: I am just going to add to that. From a data sovereignty perspective my understanding, to make sure that the Committee and we are on the same page, we are talking about the actual data being kept onshore where required and that is the proposal. Yes, I personally would support data sovereignty and I believe most members of AISA would support data sovereignty in areas where that data is of State criticality or national criticality. I would also support measures that have been taken. I go back to the GDPR from the European Union, they have a measure in the GDPR called adequacy decisions where external governments are approved for housing certain types of data under GDPR where those governments meet that criteria that they have defined under GDPR as saying, well, if as a national body you enforce these rules for your organisations, companies and government then we are satisfied that you are doing what you need to do, from a sovereignty perspective, to protect that data.

You will find that the EU has adequacy decisions with countries such as New Zealand, such as Argentina and the like. There was an adequacy decision with the US until very recently and that got thrown out because of the fact that there were some discrepancies there and they are working on that. If the State of New South Wales were to adopt that regime that would be very beneficial in that we can benefit from housing certain types of data offshore where we are happy with that but where we keep the crown jewels here in New South Wales where they belong, but we also know that data that has been outsourced is actually being protected adequately.

The Hon. ADAM SEARLE: What do you think is that critical data that should be kept onshore?

Mr VIZZA: I think personal records such as medical records which are the most coveted records for cyber criminals. That is what they are looking for. They make most of their money on the dark web through accessing those health records.

The Hon. TREVOR KHAN: Why is that? What is there that is intrinsic in health records that makes them so valuable?

Mr VIZZA: It is because of the completeness of that record. When you have a health record you have date of birth, you have blood type, you might have genetic history, you might have a bunch of different things, so as a record itself it is the equivalent of having a book that is that thick versus a one page pamphlet on somebody. For them it makes it highly valuable because they can use that data and spin it around many different ways and make some money out of it. That is why they go for it. Then you have the aspect that there is a lot of medical data out there and some of it is really poorly protected. Consider your family GP for instance, you might have a family GP that has a computer with a simple router that you and I might have at home with very little levels of protection. But they have access to My Health records federally. They have access to potential health services departments at a State level. So there is a lot of sensitive data that they are given access to that they themselves are not protecting because they just do not have the expertise to do it. The family GP is too busy dealing with making sure that they are compliant with COVID guidelines and everything else. They are just going to not do that and that is where some of the issues will come in.

The Hon. TAYLOR MARTIN: Do you mind expanding a bit more on how that record, as complete as it is, is valuable to a criminal, how is that monetised effectively?

Mr KNIGHTS: I can give you a bit of insight. If I was to be given a set of credentials, and I am thinking like the bad guys, let us put that hat on. I want to make a vulnerability. I want to build a story around how I can trick someone into believing what I am presenting is real. I can create a set of sites that are duplicates of legitimate sites. I can create emails that are coming from people that are close to that person and I may make a targeted attack about a health concern that they are deeply worried about. It may be about raising awareness or you are due for your new check-up, or something of that nature.

It may be an affiliated group raising capital, but they are trying to basically exploit that person in a way that is targeted. That is an individual level. If I look at a corporate or government level they could use a bunch of profiles to build a relationship between people where we are actually targeting a group of people and we are building a credible story that makes them believe that the story I am presenting via email, or some sort of social media, is legitimate and real. It incorporates a group of people from that association. They all start to believe that we are working with a charity or something of that nature and we start handing out details.

The Hon. TAYLOR MARTIN: That makes perfect sense. Thank you.

The Hon. TREVOR KHAN: We talk about having the data onshore. I do not travel overseas as I am not allowed or I am not given the opportunity. You talk in terms of health records. If you have a doctor who is sitting in an airport somewhere overseas accessing his patient's medical records, does it matter at that point in time where that record is housed? It seems to me that this level of connectivity creates an added vulnerability that makes geography less relevant. Am I wrong?

Mr KNIGHTS: If I talk about your term broadly it does create a concern. What you start looking at is when we are talking about how you access data and if I was to suggest that if I was accessing data remotely on a private network in an airport I would hope that the access method is a lot more rigorous than if I was accessing the same material on the office machine that is set up in the practice. What I mean by that is if I am accessing it from the phone we can put in measures that require further levels of encryption for the traffic to take place and further levels of authentication and multifactor authentication kicks in once I am not inside the office, I am out in the wide web. These are the things we talk about, and controlling that access is really important. Some of the data sovereignty things we talk about are putting an island around accessing that material and the traffic coming from an external region should go under a lot more vigour than it would if it was local.

The Hon. ADAM SEARLE: Just to talk about the issue of standards, we have heard evidence that the State Government, being the biggest purchaser of goods and services in Australia, could actually drive the development and raising of appropriate cybersecurity standards through its procurement practices. That certainly seems like a good idea. Is that something that you would agree with? Secondly, we have received evidence that there is a lack of accreditation for private cybersecurity firms, firms claiming to be able to provide onshore expertise but on investigation that is found to not be correct. Does there need to be some regulation of this kind of activity?

Mr VIZZA: In relation to the first part of that question around standards, yes. In our submission we have stated that we believe that external contractors and third party suppliers to Government should be accredited to some sort of standard. We believe that ISO 27001 is the appropriate standard. I will to some extent disagree with the previous person who was here, Professor Vijay Varadharajan, around standards. He was saying that there can be issues around standards. The way that ISO 27001 works, and I am a senior lead auditor in ISO 27001, is that different organisations can draft their own statements of applicability around what of those controls are applicable to them as an organisation, and that makes ISO very flexible in terms of a standard.

That is not to say that you can craft your own very narrow statement of applicability and then say, "I am compliant with ISO 27001." There are steps involved. You need to prove whether those steps that you have omitted actually need to be included as part of your assessment. In the past there were measures within procurement where you needed to tell Government whether you were ISO compliant or whether you were becoming ISO compliant, and I think that in the past that was quite enforced. In recent times that might have slid and I think that incorporating that back into the procurement process would absolutely be prudent by the Government.

Mr DAVID SHOEBRIDGE: It has fallen out of procurement, so we have actually gone backwards?

Mr VIZZA: We have actually gone backwards. From the latest set of procurement documents that I have seen, which was yesterday, there is mention of, "Are you adherent to the New South Wales Government guideline standards", but there is nothing around the ISO standards.

The Hon. ADAM SEARLE: That is quite disturbing.

Mr VIZZA: Yes.

The Hon. ADAM SEARLE: Although there is a body called Cyber Security NSW, it does not seem to have control of or visibility of the degree to which the whole of the State sector is compliant or is properly supervising cybersecurity across the activities of the State Government. Should there be such a central agency responsible for cybersecurity, a single point of responsibility?

Mr VIZZA: I personally think there should be and I think that the AISA would support that. In the interest of transparency, I have worked with Cyber Security NSW and provided them guidance and support. I think that they have done a good job given the level of resourcing that they have. If anything, that is a resourcing concern, which I know that the State Government has addressed by its additional funding, which is very welcome, and AISA welcomes that. I think that there should be a body that is ultimately responsible. I look at the State Government of Victoria and the cybersecurity strategy is run by the Department of Premier and Cabinet down there, and I work with them. They have a very effective method for how they manage cybersecurity and I think that we could probably learn and adopt a few of the recommendations that have come from Victoria.

The Hon. ADAM SEARLE: Where there has been a serious breach of your personal data or privacy, should individuals not have a right of action or a cause of action to get some remedy for that sort of thing?

Mr VIZZA: I believe they should. I do note that the Service NSW breach has resulted in initially some soul searching around the fact that there was a big delay in letting people who were affected know that they had been affected. I think that it was disappointing from a practitioner's perspective to see that. I think that they have made amends in terms of how they have dealt with that since, and I talked in the submission about a GDPR. There are very specific requirements around when an organisation must notify people that their data has been breached and I think that if we were to incorporate such a requirement within our mandatory breach scheme, if we do implement one—and I strongly suggest that we do—it would be prudent to list a time, a maximum number of days or hours, that an individual must be notified that they have been breached, and there must be reasonable efforts to contact that person.

The Hon. TREVOR KHAN: Do I take it that that should not only apply to government departments but suppliers to government departments? So much is done by the private sector now rather than directly by Government, so it would have to extend beyond—

The Hon. ADAM SEARLE: Down the supply chain.

The Hon. TREVOR KHAN: Yes.

Mr KNIGHTS: I might go back to your previous question about the governing body having control over the cyber maturity. I think that is important, but I also think it does not relieve the duty of care of having a cyber team in each government agency capable of doing a level of measure. I am thinking that the governing body should actually have a way of being able to report and track capabilities and make sure everyone has an action plan to actually measure up and that it is actively being pursued and followed.

The Hon. TREVOR KHAN: Is it a governing body or is it an oversight and auditing body?

Mr DAVID SHOEBRIDGE: Or is it just a policy setting body?

Mr VIZZA: It is interesting. If we look at a Federal level, the Office of the Australian Information Commissioner is actually responsible for the data breach notification piece, and that in many respects is actually almost a legal function in the sense that they have to notify by law and the like. Then you have the Australian Cyber Security Centre, which is run by the Australian Signals Directorate that manages many of the technical aspects of cybersecurity and the guidance that is provided. To your earlier point around suppliers to Government being potentially breached and having to notify, those suppliers would have to notify under the Federal scheme because the Federal scheme covers any ABN or any ACN that generates a certain amount of turnover, so interestingly they have to notify if they have been breached, but if a state government entity has been breached, or a local government entity, it does not have to.

The Hon. ADAM SEARLE: One of the examples that no doubt we will look at involved a breach involving what was then I think the Department of Family and Community Services, but they actually used Anglicare as their service provider and the data breach occurred at the Anglicare level. So the issue is that it is not a breach by FACS, it is a breach by Anglicare. Common with all of the breaches that we are going to be looking at or that might have given rise to this inquiry, the only way that those were known is because they found their way into the fourth estate, the media put a spotlight on them, so obviously any notification regime would have to extend, would it not, to all service providers to Government?

The Hon. TREVOR KHAN: But you are saying that if they have an ABN they have to report federally.

Mr VIZZA: If they have an ABN and they meet certain levels of criteria around turnover and their size and where they operate, they have to notify under the Federal scheme.

The Hon. ADAM SEARLE: Is that irrespective of whether they are providing a service to Government?

Mr VIZZA: That is irrespective of that.

Mr DAVID SHOEBRIDGE: For benefit of the transcript, both witnesses nodded after the question was asked about extending through to services by suppliers to Government.

The Hon. ADAM SEARLE: Yes.

The CHAIR: You are agreeing that there needs to be at least some oversight within departments and also across Government. Is that enough? Having sat on boards in the finance world before coming to Parliament there were requirements at board level to take cybersecurity breach notifications seriously. It became the responsibility of directors. Is it enough to have a section in a department that is looking at this or do we need to escalate it to make sure that it is at a secretary level or whoever is running the department? We need to make sure that if it is our private personal information it is taken very seriously, so should it be at that level rather than just a section in a department or an agency?

Mr VIZZA: I would say it should be escalated. Ultimately cyber risk is another risk that any organisation or department is having to deal with and the biggest challenge I think from our perspective in the past has been cyber risk, because it is something that cannot be seen, it is very intangible, is not really appreciated. I often talk using metaphors of physical security, "Would you put a lock on your door at your home?" We would all say absolutely, because we know if we do not we are going to get broken into. But then there is the aspect of doing the physical component in terms of having the mechanisms in place to prevent people breaking into the house. There is also the human aspect.

If I forget to lock my door of a morning, will I get broken into? Very likely. If I own a business and my staff forget to lock the doors and turn the alarm on of an evening before they go home, will we get broken into? Very likely. From a cybersecurity perspective it is important to have those technical controls that work and operate and do what they need to do and have oversight. But it also needs to be cascaded down to the people who are actually doing the work. I will give an example. A couple of years ago I did a presentation on cybersecurity in Victoria for a local council. At the end of it, the computer that I was using, which had been provided by council, had been locked out. I asked the person what the password was to get back in. They told me—me being anybody. The worst part of it was that the password was written on a post-it note in front of me that I had not noticed because I was in the middle of things. That is unfortunately how many people across society—and government is no exception to this—generally consider cybersecurity. That perception of what it looks like has to change.

The Hon. ADAM SEARLE: Would an appropriate model be an agency—whether it is a central agency—that sets the standards and compliance regime and audits adherence to that but that the line responsibility rests with each individual agency?

Mr VIZZA: Absolutely.

Mr KNIGHTS: Yes.

Mr VIZZA: That is where the intent behind Cyber Security NSW is to be the agency that provides the guidance and provides the assistance. At this stage I am not familiar with how much responsibility they are given in terms of mandating those controls.

Mr DAVID SHOEBRIDGE: One of the pieces you say is missing right now is even just a standard position description for the relevant officers who do cybersecurity in government departments. There is not even a standard set of qualifications or position descriptions across the Government for the people to do the job.

Mr VIZZA: To be fair, at a Federal level the *Cyber Skills Framework* that was published in September this year is that reference document. The recommendation in our submission is that the State Government incorporate and adopt that as—to your question around proper role definitions and what jobs cybersecurity people are meant to be doing and what they should have in terms of knowledge, skills and ability to help them achieve that.

Mr DAVID SHOEBRIDGE: And then we should be insisting on training people up in our State university institutions to meet those standards. So we need to set the standards and then ensure there is a pipeline of people coming through with those skills and qualifications to meet the standards.

Mr VIZZA: Correct.

Mr KNIGHTS: Yes.

Mr DAVID SHOEBRIDGE: Are we doing that second part?

Mr VIZZA: Not at this stage, no. I know that there are efforts being made but there is nothing mandated. I look to the government in Victoria, which has mandated that government employees need to have some level of accreditation and certification relevant to their job description. They have a panel of three different suppliers that departments can choose from for their people to become certified against.

Mr DAVID SHOEBRIDGE: On a different tack, the energy sector is often spoken about particularly as a potential target for other nations that might want to target our economy. The energy sector is repeatedly referenced as a target, at least in media commentary. Would it be accurate that it is a vulnerable or attractive target if you want to take down an economy?

Mr KNIGHTS: Well, the answer is yes. It is very spectacular. From a nation-State, if they want to do something spectacular and attack at a nation-state level, they will target key infrastructure. The sophistication that we are talking about for those types of things is really at that nation-state level. I think some of the broader things that we are talking about are not at the nation-state level, but we still have to be mindful that those threats are there.

Mr DAVID SHOEBRIDGE: As we have a more decentralised energy sector—literally power being fed into by hundreds of thousands of homes across the State, all of those constant interactions—how do we ensure that all of those devices that are feeding into our energy sector have that the kind of cybersecurity needed? Is that an area of vulnerability that we should be right now setting minimum standards for cybersecurity on those devices?

Mr VIZZA: Absolutely. I am happy to take this on notice because I do not have the details to hand, but Very recently there was a provider of solar panel products that had connectivity. A major vulnerability was discovered in those solar panels that effectively gave a cyber criminal full access to their home network. That organisation was approached and the first thing they did was get a lawyer to claim—

Mr DAVID SHOEBRIDGE: To shut them down?

Mr VIZZA: Yes, basically that there was slander involved in the claims, even though the claims were legitimate. As a result of that, there were some significant problems.

The Hon. TREVOR KHAN: Would you like to explain that a little bit more? Is this an issue with regards to individual financial vulnerability or is it vulnerability of the network to State actors?

Mr VIZZA: In this particular instance, my understanding of the issue was that the particular product was vulnerable to external access and, therefore, gave someone full access to their network and whatever might have been involved.

Mr DAVID SHOEBRIDGE: Just stopping you there, that is access to the home network, not the broader infrastructure network?

Mr VIZZA: To the home network. However, if those devices were used in a commercial environment then it goes without saying that you would have the same sort of problem in a commercial setting. In our submission we stated that we believe that there should be controls around products in terms of having minimum security standards for products. The state of California in the United States has implemented a law, which is the IoT security law. They talk about things such as making people change their passwords the first time that they install it and making sure to turn on things such as two-factor authentication. That is effectively where you have a password to log in but before you can fully log into the system you have to provide an additional bit of data, which is usually provided to you by text message.

The Hon. TREVOR KHAN: By your phone.

Mr VIZZA: Yes. That verifies that you have what you know but you also have what you need to have in order to access the system. There are a bunch of different recommendations and I would suggest that the Government look at that California law because that will end up driving much of the reform in that space.

Mr DAVID SHOEBRIDGE: It seems to me there is a degree of urgency in at least that space because we are constantly installing those systems. And that is a great thing; The Greens 100 per cent support it. But I am astounded that there is not a minimum cybersecurity requirement for those home installations.

Mr KNIGHTS: Yes. I think one of those things is that it has been to market. People are commercialising products and sometimes they do not have the expertise and we are not holding them to a standard that they need to acquire those expertise or at least outsource those expertise in code writing or product software. We are in a state where we are releasing products to market and reinventing the same mistakes that we have made by not holding them accountable to a certain standard to allow them to enter the market.

The Hon. TREVOR KHAN: So many of the products, if you look at solar panels, are imported, and imported from particular locations. We cannot really teach those manufacturers in those locations how to do it better. There has to be two questions. One is that we really have no quality control over what they are doing. The second thing is that in some cases we are not, perhaps, aware whether or not the chip they are putting in is vulnerable for nefarious reasons. That is a problem, is it not?

Mr VIZZA: The biggest challenge of IoT security—and we talk about IoT as a category generally—is that we all know that we need to update our phones and our computer software because, if we do not, we will have certain issues. The problem with IoT devices generally is that it is very difficult to update that software. You might ask, why would I want to update the software? Because over time we discover vulnerabilities in bits of software and we have new ways of getting into systems and the like. As a result, if we cannot update that software, we end up having products that are vulnerable and susceptible to issues. That is a major challenge and that is where this IoT reform, particularly in California, looks to address that, in that they have to provide a capability to update that software.

Mr DAVID SHOEBRIDGE: I am monitoring just now my house's solar output and the battery charge. I can do that on my device but I have no idea where that data is going apart from in my phone. I have no idea if that is sitting in the cloud somewhere. I happen to know the country that manufactured those solar panels since it is not Australia; I do not know where that data is sitting. I do not know how vulnerable it is. I do not know what the protections are.

The Hon. ADAM SEARLE: Maybe that is an example of critical infrastructure data that should be retained onshore.

Mr DAVID SHOEBRIDGE: I suppose that is the question.

The Hon. TREVOR KHAN: It is not simply the data.

Mr DAVID SHOEBRIDGE: It is the access into the device.

The Hon. TREVOR KHAN: It is the access.

Mr VIZZA: Creating a Smart world is something that we all think is great and innovative, and everyone has got that.

Mr DAVID SHOEBRIDGE: I am feeling a bit dumb right now about my—

Mr VIZZA: The challenge we have is keeping systems updated, and looking out for these vulnerabilities and have a social conscience that this is what we need to do. I think what we are talking about from a standards perspective is having an entry point that says you at least need to adhere to this level to be in the market. At the moment we are not excluding people that have not measured up with a measure. We want to start with a starting point, allow people to say "This is the hurdle you need to actually reach to get into the market." And from there we can actually refine that and raise the bar over time as we get more sophisticated with how these devices are interacting with our life.

The Hon. TREVOR KHAN: Maybe it was not sufficiently transparent but is the problem that arose with Huawei in terms of setting a standard in terms of the 5G network, that they just continued to argue vehemently that the standard that we set and the vulnerability that we say was identified does not exist? If we wind this out even further one of our problems is going to be, is it not, is that we will be confronted with an allegation that we are not setting a standard for cyber security, we are simply creating a trade barrier? I think that seems to me to be where this is all going to end up, is it not?

Mr VIZZA: Yes, and it is an interesting counterpoint. In cybersecurity, like with anything, you can create a system that is fully open and has no security controls and it makes it ultimately the most accessible, usable system that you can have or you can create a system that is so secure that it is inherently unusable. So much of what we are trying to do is find that sort of balance between where is the appropriate level of functionality provided? Where is the appropriate level of security also provided?

To Stephen's point around setting standards, standards should be seen as a baseline in terms of "these are the minimum levels of hurdles that you need to jump through for these products to actually go to market". I think if that causes a trade barrier then I think that is a concern from a commercial perspective purely because of the fact that, yes, organisations need to make money and the like but also they need to provide safe products. We would not tolerate unsafe products being sold in other areas so we should not—

The Hon. TREVOR KHAN: But we do. We have cladding all over buildings.

Mr VIZZA: Yes.

The Hon. TREVOR KHAN: I perish the thought I have raised that but we have cladding all over buildings because our system of trade is that whatever comes in on the wharf, essentially as long as it is not full of drugs, there is no checks and balances that state that before a product goes to market it has to be certified as complying with an Australian standard.

The Hon. ADAM SEARLE: And yet you do for medicine and stuff like that. It is quite interesting, isn't it?

The Hon. TREVOR KHAN: But that is a true exception.

Mr DAVID SHOEBRIDGE: Motor vehicles have standards. It is possible to impose standards it is just that we haven't and it makes us more vulnerable.

The CHAIR: The recommendation here is that we should. We are out of time.

(The witnesses withdrew.)

(Short adjournment)

TONY VIZZA, Director, Cybersecurity Advocacy ISC2, on former oath

MICHELLE PRICE, Chief Executive Officer. AUSTCYBER, Australian Cyber Security Growth Network Limited, before the Committee via videoconference, affirmed and examined

JUDY ANDERSON, Government Relations and Advocacy Lead for AUSTCYBER, before the Committee via videoconference, affirmed and examined

The CHAIR: I welcome our next witnesses. You are welcome to make an opening statement if you would like.

Ms PRICE: The significant digital uplift across the economy and particularly of course, because of the pandemic, is placing pressure on our digital network services and activity. Creating trusted digital services, including ensuring our cybersecurity posture and capabilities are designed to protect, secure and better resilient has never been more important. The New South Wales Government is taking significant steps in this direction through its $240 million investment in cybersecurity across its government networks and services. In this regard, we believe that on cyber the New South Wales Government is taking a leadership position nationally that sends a clear message and is showing the way for governments across Australia. This is not just for the Federal and the State and Territory levels but also it is for local governments around the country.

The focus of the New South Wales Government on designing procurement arrangements for ICT and digital technologies that encourage fulcrum procurement is a part of this important step. In relation to cybersecurity, its investment and incentivising fulcrum biosecurity capability to be the best investment in keeping our digital activity secure is a position of leadership of the sovereign State contributing to global competitiveness of the economy of New South Wales but also to the economy of the nation. I also want to note for Committee members that at AustCyber we do a lot of publication of material that is actually often globally for the first time. One of the documents that we produce annually is the Cybersecurity Sector Competitiveness Plan which you may have seen. It provides a huge amount of data on the nature, shape and size of the sector as well as the size of the opportunity for the Australian economy if we are secure in the technologies that we build into the performance of the economy.

We also focus significantly around cybersecurity skilling. It is a requirement of our contract with the Commonwealth of Australia that we focus on these areas. It is also a requirement that we focus on regulatory reform, and have done significant work over the years with the Australian National Audit Office and the New South Wales Audit Office as well, and that includes Audit offices around the country. Within the context of cybersecurity part of what we are doing right now is working on the 2020 update of the Sector Competitive Business Plan. It will adopt the position that will take Australia into the international landscape around how to thrive and be categorised by the security capability.

We have aligned this characterisation with the international collaboration that is happening out of the UK around a cybersecurity body of knowledge or BOK. These are documents that help guide the left to right of industries. The most famous BOK that exists in the world, of course, is the engineering body of knowledge. Australia is contributing significantly to the cybersecurity body of knowledge. Within that body of knowledge it describes five different capability categories and within that 37 capability types. So that is really important to understand the breadth and depth of the challenge that is faced by the economy in truly understanding the complexity of cybersecurity.

I also note that Tony Vizza referred earlier to cybersecurity skills framework. We have been pushing the United States National Initiative for Cybersecurity Education workforce framework. It describes 14 job types and 52 job roles in the industry of cybersecurity, and that also supports employers to understand how cybersecurity is now an element of every job in the economy. That framework has now been adopted as the base of what the Federal Government has been doing around cyber skilling but it also has been increasingly adopted by government agencies as part of their attraction and retention policies in cybersecurity skilling for their agencies. We have been doing that work in partnership with Cybersecurity NSW. I will leave my opening remarks there. Thank you.

The CHAIR: Mr Vizza, do you want to make a brief opening statement?

Mr VIZZA: Madam Chair and members of the Committee, thank you once again for the opportunity to provide input into the Legislative Council inquiry into cybersecurity. My name is Tony Vizza. I represent an organisation called (ISC)2, an international not-for-profit membership association of over 150,000 certified cybersecurity professionals around the world, with over 1,200 members based in New South Wales. (ISC)2 advocates for a safer and more secure cyber world and welcomes this inquiry. As you may be aware, matters related to cybersecurity have achieved significant prominence in New South Wales in recent times. In

July of this year, Prime Minister Scott Morrison illustrated the eroding cyber threat environment. This followed a number of high-profile breaches that occurred across Australia and in New South Wales, both at a private and public sector level. Federal agencies have registered just short of 60,000 reports of cybercrime over 2019-20 at a national level. This is a huge number, comparable to and even exceeding categories of traditional property crime, such as larceny.

These trends are not unique to New South Wales. In the UK for example, cybercrime is now the number one category of reported crime. I can further cite a veritable pile of studies, reports, white papers and the like that illustrate beyond any reasonable doubt that cybercrime is now a top three global concern, right up there with the likes of global pandemics and climate change. We now come to the question of what we as a State can do to deal with the issue of cybersecurity and cybercrime. Cybersecurity is entirely reliant on three pillars to ensure good outcomes can be achieved. The first pillar is an understanding that people are the most essential ingredient in any successful cybersecurity strategy. This involves ensuring that people are aware of the risks, appreciate how those risks can impact their day-to-day lives and take proactive steps to prevent those risks from eventuating.

It involves ensuring that professionals tasked with protecting the information assets of organisations and government are competent, skilled and certified in being able to do so, which is a significant element of what (ISC)2 strives to achieve. It also involves ensuring that these people have access to relevant resources, training and skills that help to provide timely information in an industry that changes by the second. The second pillar is understanding that process needs to exist when seeking to implement strong cybersecurity measures. Many of the items listed within the terms of reference in this inquiry relate to process. The adoption of industry standards for the management of information security systems is critical. Many of the recommendations in the submission discuss this pillar.

However, it is vital to emphasise the point that without the people in an organisation possessing the right levels of skills, knowledge, experience and mindset, any attempt to create processes that minimise the risk will be flawed from the outset. We know this to be self-evident. Consider, for example, mature industries such as aviation, where there is no question that best practice dictates that the people working in the sector are competent, skilled and accredited. The third pillar is technology. We all know that this is a high-tech sector. However, once again I should emphasise that the technology functioning as is intended is entirely dependent on the fact that people are duly trained, skilled and accredited to deploy, manage and maintain that technology to begin with. It is the hope of (ISC)2, and my personal hope as a citizen of our great State, that the recommendations made via the written submission and my testimony here today will result in a safer and a more secure New South Wales. Thank you.

The CHAIR: Thank you very much. I am happy to start with AustCyber. Your big push is for the State to build some sovereign cybersecurity capability. You talked a bit about that in your opening statement, but can you expand on why that is important? Also, referring to your submission, you suggest that there should be some minimum requirements of five per cent with a target between 15 and 25. How much capability do we have now, and what would it take to get there?

Ms PRICE: AustCyber's mission is to be able to create a globally competitive cybersecurity industry for the nation. Over 50 per cent of the sovereign companies that are currently within Australia—of which we look after over 350 and we believe there is around 500 in total, so we still have a way to go to reach all of them—are currently sitting within New South Wales. The data around that is going to be published as part of the 2020 update to the AustCyber *Sector Competitiveness Plan* this year. We have taken a deep dive into the State's approach to the economics of cybersecurity for each of the jurisdictions, but New South Wales is a high performing market and there is a whole range of reasons for that. The reason sovereign capability is so important in cybersecurity is because of the role of digital trust, and the fact that humans do need to have some sense of trust around the technologies that are being used to help secure the environment in which they operate.

Sovereignty is not just an important aspect for national security in that traditional sense of what national security is as it applies to all jurisdictions, and the contribution that New South Wales makes to the nation's security, but also for economic security. Sovereignty in the equation of cybersecurity is all about those geopolitical issues that we hear so much about in the national and international media. Being able to trust the technologies that we deploy to defend against malicious attacks on digital infrastructure and the data that it carries is critical. More than that, we need to be able to have our stake in the sand to be able to sustain the economic growth that we are now relying so heavily on, particularly in pandemic recovery, around the creation of new industries and the jobs and revenue that come from it. A lot of that is in the technology spaces, as the Committee members would know. Being able to trust the creation, commercialisation and scaling of those technologies has become critical.

The investment of other nations into these is actually off the charts. We know that Australia is quite behind when it comes to marking out our own territory in this kind of way. We are one of the last western nations to focus on it. Having over 500 sovereign companies within Australia, and having a good chunk of those within

New South Wales, is really only the start of what we need to do to be able to retain the trust within our digital systems.

The CHAIR: How do we get to the recommended percentages that you talked about? How can the New South Wales Government help with that? What kind of investment do we need? I understand the argument about jobs and building an industry here, but what would it take for the New South Wales Government to support your suggestion for this?

Ms PRICE: I am really pleased to report to members that AustCyber has been contributing significantly to the New South Wales Government's ICT/Digital Sovereign Procurement Taskforce. I believe that the outcomes of that task force, which finished its work three weeks ago, is currently making its way through the Cabinet process. Speaking to Mr Vizza's three-pillar matrix, the kinds of processes and people that are needed to make that work, to provide assurance to government systems and services is a focus on making sure that the Government proudly and transparently provides opportunities for innovative cyber capabilities to be procured from.

Government is the largest lever in this space, both for the assurance of the management of cyber risk as well as for that jobs and growth side of things. So the kinds of work that has been going on within that task force gives me great assurance that we are actually going to be able to make headway in this space. The really important part in all of this is the culture of procurement. Being able to provide the right incentives within the system that rewards procurers and decision-makers to support the system that is likely to make its way through Cabinet and out into government agencies, and the changes to the policies that will happen around that. We need incentives that will reward people to change their behaviours to create a mix of providers in the system.

Those providers need to be trusted through mechanisms that we have been talking to Cyber Security NSW about, like using what is called a procurement sandbox, that de-risk the ability of government agencies to be able to procure from vendors that have not previously been procured from. Particularly when it comes to small business, the old adage that you need to make sure that the company is still around tomorrow to be able to procure from them is actually a perception and it is a myth that we are working hard at AustCyber to bust. Very few cybersecurity companies go bankrupt or go out of business these days, and a lot of what has been provided into the market is pretty high quality. So we believe that, as long as the culture can be fostered around shifting behaviours in decision-making and procurement processes, we will see that target and more delivered on.

The CHAIR: In terms of the sovereign cybersecurity capability, you mentioned that we are one of the last remaining Western countries not to have looked at this or started on it. Is it too late? If we create a capability here is it easy for government agencies, other agencies and businesses to move their storage or are we too far behind?

Ms PRICE: I would say that it is not easy but it is straightforward. Again, in the Sector Competitiveness Plan we outline what the barriers are to be able to achieve that step up. Removing those barriers mostly comes down to matters of culture but also matters of awareness and understanding. The way that the New South Wales Government has gone about providing those leadership positions and the investment that it is currently making to address the gaps highlighted by the Auditor-General's report and other areas of investigation is a very strong step forward. We have to recognise, though, that time is needed for a holistic set of outcomes to be achieved.

What has happened in other places in the world that have recognised that they need to step up is a co-investment of time, money and resource—from a people point of view—to be able to have focus and energy put into how to raise the tide, so to speak. I think that Australia has been making good efforts but we really do need to have that sort of leadership taken to really step up and move up the pack, if you like, around recognising just how central cybersecurity capability is to the economy now. Being able to foster sustained growth within the cybersecurity industry that provides those products and services in a globally competitive way is critically important for us to hit our goals as a jurisdiction of New South Wales, but also for the nation, around pandemic recovery and economic growth longer term.

Mr VIZZA: I will add some comments to Ms Price's comments here. If you look at nations such as Israel and Canada, for instance, they have dedicated a significant percentage of their government mindshare into making sure that they are on top of this. To Ms Price's point, I think that we might have made a slow start. At (ISC)2 we fully support the work AustCyber is doing and we think that it is highly valuable. It obviously gives us national sovereign capability and State sovereign capability, but it also gives us some international competitiveness around some of the things that we can export and provide overseas. But we need to make sure, of course, that what we provide is valuable and secure. We come from a perspective of making sure that the people in these organisations have the relevant knowledge, skills, abilities and experience to create products and services that are secure by design. I think it is really important to note that that is where we come from, from this perspective.

Mr DAVID SHOEBRIDGE: In terms of digital trust, data sovereignty is one of those core elements. Is that right?

Ms PRICE: It is one of the key components but it is not the only component. One of the challenges that we have experienced in Australia around the topic of data sovereignty has been the different sets of understanding around what that actually means when we do have a hyper-connected economy. As much as we do not necessarily understand the technologies that we are using—and certainly we seem to be very quick to buy foreign technology in the country—the piece about data sovereignty can be challenging to manage but it relies on trusted relationships. It can be done and we need to recognise the layers that happen around data creation, transfer, ownership and sustainment. We need to be able to understand that there will always be challenges within the infrastructure that carries and holds data that mean that we will not always be sovereign.

That is why a trusted ecosystem of partners is really, really critical. We know at that really big-hand level that those relationships are already in place through mechanisms such as the Five Eyes. Australia does enjoy some of those kinds of benefits but often they are actually limited to the Federal Government. We need to make sure that similar kinds of models are available to industry, including the small end of town, to be able to understand what is truly important for data sovereignty, in terms of what parts of the data and data creation and maintenance process is critical to retain on our shores versus the parts of the process that are perhaps not as critical. If they are going to go offshore, where are they going and what kinds of controls do we have over the location and the infrastructure that is holding it?

Mr DAVID SHOEBRIDGE: Can I give you a very real-world example that has been playing out this year? Much of this is partly a response to COVID-19. An array of regional universities and major city universities across the country have gone to online proctoring. The examinations are taken online and as the students are sitting and doing their exam, they are being randomly observed through their laptops to ensure that it is only them in the room. Sometimes they have to pass the camera around to show that it is just them in the room. All of that information is being taken to an offshore proctoring service.

Often coupled with that is all of the facial recognition data that the university has to ensure that the student in front of a laptop is the student who is registered to do the course. That is a huge amount of data that is being offshored at the moment through a variety of separate commercial arrangements that have been entered into by universities. I am unaware of any basic standards being put in place for data security. Can you talk to that as a current industry example?

Ms PRICE: I think that it is a fantastic example, so thank you for raising it. It is representative of what is going on across every segment of every sector in the economy. As serious as that is, it is real. Even if we did not have the pandemic circumstances forcing a lot of this activity online, it would still be representative of what is going on in the economy writ large. It has a lot to do with the economics of it. The services that are provided by the very large multinational cloud providers particularly make it very attractive during circumstances under pressure—such as what you have described—to go with their model, rather quickly than in an informed way and considering what the risks might be for just accepting a service on face value and not asking any questions about privacy and security.

That is absolutely a great example of where there need to be questions asked of the provider as to how data is going to be managed, secured and sustained. As the Committee would be well aware, no data can actually ever be deleted. There are data mechanisms that can be destroyed but no data can truly ever be deleted. The General Data Protection Regulation in Europe obviously deals with aspects of that. In terms of those data standards, we do not have them in Australia. But from the business of doing cybersecurity in Australia, we can take some cues. Even if there were regulations and standards around those kinds of elements of how businesses, including universities, need to go about securing their data, the practice of it is what is most important.

Providing the right incentives to show what "good" looks like and step organisations through the benefits of measuring those risks and taking risk-based decisions is critically important. It really does happen across so many different elements of everybody's day. Having some signals in the market around what "good" looks like is a role that Government can and should play. I might note here that obviously the lens has been put pretty sharply on the university sector for lots of reasons over the past nine months, including around their cybersecurity habits. There is not very much available for universities at the moment to actually help them do this well.

We at AustCyber have funded two projects to help at the infrastructure level and we are trying to work through an information management point of view on the data side of things as well. That is through the group of eight universities; not through the group of eight itself, but for members of the group of eight, to be able to show the rest of the value chain what good looks like in this space. When you are faced with that very quick decision you will probably go for the thing that is at the top of your email queue that sounds okay and provides what you think is good value for money because it is cheap but actually the value for money is not there, the cheapest option is not the right option.

Mr DAVID SHOEBRIDGE: You only have to think about the reputational damage and then the commercial damage that would flow if there is a substantial breach and, for example, a whole cohort of students' facial recognition data is lost. Those costs, are they being factored in, to your understanding, in the commercial framework at the moment?

Ms PRICE: In some organisations they are. It would not surprise members that the more mature organisations within the economy, which happen to be the regulator sectors traditionally—financial services, telcos, a lot of the health industry, although not all—do take these kinds of factors into consideration. The chief information security officers of those organisations are often under significant pressure to justify to their senior executives and their boards why they are paying more for a product than what the cheapest available product is and, of course, it is because of that risk consideration.

It is often that under education of decision-makers, whether they be senior executives and boards, or councils in the case of universities, and low understanding around what those risks are that really belies the opportunity to value those risks appropriately. I do think that one of the key things for Australia is to shift our understanding of what value for money is now. We are living in a cyber-physical world. Those traditional concepts of what value for money is, which in the Australian economy, as you know, has been traditionally dictated by government procurement processes, that value for money equation is now well and truly out of date. It has exposed us to enormous vulnerability and risk.

Mr DAVID SHOEBRIDGE: You talk about education and setting good standards, but particularly when it comes down to offshoring personal data do you think there is a place for minimum standards to be regulated for all significant institutions if they are offshoring personal data from Australian citizens, Australian residents, Australian businesses, that there is a place for government to set minimum standards for the protection of data in the offshoring context?

Ms PRICE: I think there is and another related task force to the procurement task force that AustCyber actually chaired for the New South Wales Government in the middle of this year was a cybersecurity standards task force which is around providing what "good" looks like for minimum baseline standards across different industries, which phase eight industries to focus on in the first instance. And we are going to be working with Cyber Security NSW and Service NSW to cover off the rest of the sectors that were not addressed in that task force. That work is now feeding up into what is called the Better Regulation Task Force that has been established under the Department of Home Affairs under the National Cyber Security Strategy released in August. Of course, as part of that cyber security strategy the country is about to see new definitions of critical infrastructure come into play.

The Minister for Home Affairs is expecting to table draft legislation before the end of this calendar year on new critical infrastructure regulations and legislation around cybersecurity in critical infrastructure. Part of that is going to be about data sovereignty and data retention requirements. I do not mean retention in the sense of that legislation, I mean retaining data onshore and if it does have to go offshore how do you manage that? I do think though that there will still be a significant requirement for State and Territory governments, and New South Wales is in the box seat to lead here, to provide the kind of translation of that legislation and regulation down into small business. Small business in value chains, as we know, are incredibly exposed to not having the right kind of information and not having the right kind of advice to be able to implement these kinds of practices effectively.

We are working really hard at AustCyber to remind all of the people involved in creating these kinds of regulatory landscapes that we cannot just create these regulations and legislation for the big end of town who have the resources to be able to lobby governments. It is actually the SMEs, but more importantly in that SME equation it is the small businesses, including start-ups, that usually do not have the capacity but often have the innovation to help solve some of these challenges. Value chains, as we know, are becoming more and more lucrative. They are also a very, very sharp target for malicious cyber activity.

The Hon. TREVOR KHAN: I just want to pick up on the issue of cyber security standards. You have talked about some of it already. Can you talk to us about the harmonisation of those standards across Australia and what is going in that space?

Ms PRICE: Thank you for the question, it is a great one. Why did we pick New South Wales? It was because we felt that at AustCyber the way to actually drive some change and to enhance the conversation around harmonisation to be able to reduce the transaction costs involved in doing business rather than increase them was to go after the biggest economy within Australia and the one that was most conducive to understand the complexities of how to do the practice of cybersecurity well and that is New South Wales. What we have been doing as part of the work with New South Wales Government in the area of standards, it is absolutely about providing a baseline across all industries.

What is common across all industries is to then have the contextual need in each of these standards areas for industries that build on that baseline. Concurrent to the work that we have done with the New South Wales Government, we have spoken to every other jurisdiction in the country around dovetailing off the back of the work that we are doing in New South Wales. We are doing that in partnership with Standards Australia so that we also have an eye to the international standards landscape to leapfrog some of the things that we have left behind or we were falling behind on in Australia, to be able to leapfrog straightaway into a situation where we have an agile framework that can adapt not only to new technologies but also malicious behaviours and the international standards landscape, which members might be aware is still a bit of glacial activity around what cyber standards look like.

Again, New South Wales can be a force multiplier for the whole of the country in terms of harmonising those standards with the kind of pushing up, applying the right kind of pressure up into regulation but also at the same time addressing global competitiveness and for Australia to be a modern model for other countries around the world to then follow as well.

The Hon. TREVOR KHAN: You used the word "can" on a number of occasions when answering, is the New South Wales Government taking that lead?

Ms PRICE: I think it is. Where the hold-up is in the timeframe of putting things into action is not sitting with the New South Wales Government, in my view, it is actually sitting with the Federal level. In speaking in full frankness the New South Wales Government really has been providing leadership on this and has come out ahead of the Federal Government. The feds are not particularly happy with that because, of course, they believe the domain of standards and the way that you set what good looks like should sit at the Federal level because they are the ones that supposedly owned the story internationally. It is not actually true. We have actually been the honest broker in between the two parties in that regard to be able to smooth out what the true thing is that we are trying to achieve.

What is the actual outcome that we need to achieve? Let us put aside the competitiveness in that negative way of the Federation and let us actually look at the positives of New South Wales providing an amazing use case for the rest of the country. The other States and Territories are super keen. They are willing and ready to dovetail in and that is not just at the officials level, that is at the political level in every jurisdiction. It is now just making sure that the Federal Government is not a fly in the ointment of their position in the landscape, this is actually doing a lot of hard yards work for them that they can take the credit for internationally.

The Hon. ADAM SEARLE: We are getting a fairly good impression of the risks, as well as the opportunities, in the cyber space and from the oral evidence we have heard this morning and from the written submissions it seems that at least part of the solution rests with having proper standards set for Government to comply with by some sort of central cyber agency in government and for those standards also to apply to those providing services to Government, and that Government should use its procurement buy, as it were, to drive the development and the lifting of standards in cybersecurity across the supply chain. Does that seem like a reasonable step to be taken?

Ms PRICE: Absolutely. I back that 100 per cent at AustCyber. I have done a lot of work with Governments internationally who are very curious about the model of AustCyber, and that has given us the opportunity to have insight into how those Governments are approaching this issue of how you actually push behaviour in the right direction, leveraging the position that Governments hold in value and supply chains, but also to make sure within that equation that Governments' own systems and services are cyber resilient. We also do a huge amount of work at AustCyber with the World Economic Forum, so when you take that industry lens and Government lens this absolutely is not only the most efficient and effective way to drive the outcome; it is also the quickest way to drive the outcome that we are trying to achieve here, which ultimately is for the people of New South Wales to have trust in the cyber resilience that is trying to be achieved within Government.

The Hon. ADAM SEARLE: The two additional steps that have come through fairly clearly in the evidence we have had so far are mandatory notification of data breaches to ensure ongoing public trust rather than people finding out when they open their newspaper, and data sovereignty capability in terms of crucial data, not just located in Australia—and I think Mr Khan raised this earlier—to ensure that there is security about how that information can be accessed. Would you agree with that?

Ms PRICE: From my perspective, yes. I think the tweak that I would make to that as an addition is that the culture around breach notification again needs to have some injection of what good looks like. Breach notification should not be taken as something that is a slight against the ability of a company or an agency to be able to do cybersecurity well. I am sure that within the evidence that you have received so far members would have noted that this is a journey. The game of cybersecurity is ongoing and the arms race is getting pretty sharp. If an organisation, whether it be public or private, discloses mandatorily that it has been breached and/or compromised, we should have a culture of not sort of throwing bricks at those organisations; we should be rallying around them to help them resolve that situation and learn from it so that we can continue to build the resilience of the systems overall as well as the culture that surrounds it all.

We have seen this happen in locations internationally where there are incentives that are built into the system for the humans to reward people to notify, even if that is required under law mandatorily to disclose, but actually that that is rewarded, that it is seen as a positive, it is seen as a learning opportunity, and it is something that we can all provide some help on. When I think about some of the significant breaches that have happened in Australia, including in the New South Wales Government, the context of these breaches is really important for the public as well as other organisations around that organisation that has been breached to understand. The context of malicious cyber activity is very complex. It can be random, but often there are patterns that are involved.

If you look at the time from when the New South Wales Government disclosed to the public that it was going to be focusing on cybersecurity and that it was going to step up its game around cybersecurity to when some of those more recent breaches occurred, there is a pattern there. Every time anyone says that they are good at cybersecurity or that they are about to embark on a journey of cybersecurity, malicious actors will go and have some fun, so it should not necessarily be seen as a negative. Absolutely we need to see what has happened within those breaches and how we can do better, how we fix and remediate, but we should not be throwing bricks, in my view, because that actually serves to undo the very purpose of what mandatory notification is all about.

Mr VIZZA: I would like to add a couple of comments.

The CHAIR: Just before you do, would you not say that there is a fairness trade-off that is required? Sure, we should not be throwing bricks and we should welcome openness and accountability, but that means that the Government agencies have to be open. There is no mandatory requirement now, which means we do not know what breaches there have been. It is well and good to say that there is a little bit more disclosure if we are now talking about cyber, but we do not know what other breaches and incidents have occurred with our information or within Government agencies. It is also probably fair to say that for us to welcome Government disclosing this information and having better processes in place to fix it would require timely reporting to the community, not months later via snail mail on a drip feed. Would that be fair enough?

Ms PRICE: That is fair enough. I think that again when you look at the good models of mandatory notification around the world there is a very key principle of transparency that is the foundation of those systems and I would encourage you to have a look at the model that is in play—it is almost 10 years down the track—in California in the United States where they have learned some really hard lessons around how to do this well. In terms of time for disclosure, that is a really tricky one. Certainly if Governments do put the investment into having the eyes and ears on the ground and in the systems around what is happening in the infrastructure and the data to be able to know what is going on, knowing what is happening in a system is really important, because often the delay is because the agency itself has not known for a really long time that it has been breached or compromised.

In Australia at the moment the average time from the actual breach through to an organisation knowing that they have been breached is 286 days, and that is often because they do not have sufficient monitoring of their systems and their infrastructures. We need to remember that it is not just what is within your own perimeter, what you actually own yourself; it is also the systems and the networks that you are interfacing with as an organisation, again whether you are public or private, so there are very good reasons why often there is a delay, but if we put the investment in to having that monitoring and understanding of what the data is telling us, then absolutely that can speed up—and transparency is key.

The Hon. ADAM SEARLE: You said earlier that you cannot ever delete information. What did you mean by that? If I delete my email, surely it is gone?

Ms PRICE: I am afraid it is not.

The Hon. ADAM SEARLE: Really? Please tell us some more.

Mr DAVID SHOEBRIDGE: Why don't we be more specific. If you delete a Word document, what is left?

Ms PRICE: The metadata is left and, of course, when you delete it, it goes into your computer's cache, what we know commonly as the recycle bin. Windows has taken out the recycle bin, but you can actually still find it on your system if you know how to get to it, and if you know coding then you can pick up the traces of the code behind every email, behind every Word document, Excel spreadsheet, behind every application. It is often the code that malicious actors are going in to find, and anyone who has the skills can re-engineer it to put enough information back together again to know what was actually in that communication or document. So it is incredibly difficult—incredibly difficult—to truly destroy data.

The Hon. ADAM SEARLE: So if the Government deletes an email or a Word document, it can recover that information if need be?

Ms PRICE: That is right, yes.

Mr VIZZA: Absolutely.

Mr DAVID SHOEBRIDGE: You said "absolutely", Mr Vizza?

Mr VIZZA: Absolutely, yes. To give you some context from a technical perspective, we would recommend if someone is looking to, say, delete all contents on their hard drive, to format their hard drive seven times using very sophisticated technologies that will effectively erase every bit of data on that hard drive, and do it seven times.

Mr DAVID SHOEBRIDGE: That is more effective than a tractor?

Mr VIZZA: You can use a tractor, or shred the hard drive.

Ms PRICE: To spin off that, particularly with cloud storage of data, because a lot of data is now being stored in the cloud, and of course there is secure cloud that is being used, which is wonderful, a tractor will not work.

The CHAIR: Indeed. Thank you for your time today. We appreciate the evidence that both of you have given us today. Thank you for your work.

(The witnesses withdrew.)

ANDREW COX, Member, Steering Group, Active Cyber Defence Alliance, sworn and examined

HELAINE LEGGAT, Member, Steering Group, Active Cyber Defence Alliance, before the Committee via videoconference, affirmed and examined

The CHAIR: You are each entitled to make an opening statement if you would like to.

Mr COX: Thank you. First of all, thank you for the opportunity to address the Committee. I am speaking on behalf of the Active Cyber Defence Alliance, which is a special interest group comprised of industry, academic and government stakeholders, whose aim is to foster active cyber defence practices with the goal of lifting Australia's cyber resilience. We adopted the term "active cyber defence" from Major General Marcus Thompson, Australia's head of information warfare, who rarely speaks in public without calling out the importance of active cyber defence.

By active cyber defence we are referring to cyber intelligence, deception, active threat hunting and lawful countermeasures to give defenders visibility of their adversaries' objectives, methods and identities so that they are no longer fighting blind but can predict, detect and respond effectively to malicious cyber activity, as against conventional or passive cyber defence measures, which are basically those recommended by the other submissions to this inquiry. We recognise that those are necessary but they are insufficient, particularly against motivated and skilful adversaries.

Despite the large investment in new technologies, procedures and operator training that has been going on across the industry over the past so many years, the Ponemon Institute in the United States research found that, across America enterprises, about 210 days is the average time it takes to detect a breach. We just heard a statistic a moment ago that it is 280 days in Australia, so we are well behind the curve. This is not including small businesses, this is American enterprise, which are arguably ahead of us in terms of cybersecurity adoption. What is even more bothering is that 66 per cent of breaches are not detected by the victim; they are detected by outside parties. So the methodologies that are being used are not working effectively. That is a long time to have an adversary loose in your environment without you even knowing that they are there.

Essentially what is going on is that we are like a blind boxer in the way that passive cybersecurity works. We have our eyes shut and our ears blocked so our opponent can beat the living daylights out of us. We flail around trying to defend ourselves and once in a while we land a lucky punch. By and large we on a hiding to nothing. If we can open up our eyes and start to see the threat environment—not the generic threat environment that is affecting everybody but what is affecting this or that organisation specifically—and detect activity effectively, then we will have the ability to exact a cost against our adversary and make ourselves a far more hostile target.

Our Federal agencies, particularly our Federal security agencies, understand this very well and they use cyber deception and intelligence tools as part of their day-to-day practice to defend themselves. They keep that trade craft very private and do not share that information. A number of us who work in the industry have joined together with the mission of breaking the trade craft of active defence out into the general civilian, government and private sector industry. I must say we have quite strong support across various State and Federal government jurisdictions and organisations, as well as private practitioners. Our advice, particularly, is to grasp this opportunity to take a step forward in terms of our cyber resilience by mandating that State Government agencies in their annual cyber drills start to explore and test some of those tools and methodologies to get their feet wet and begin to appreciate how they might improve their cyber posture, rather than push them off as some exotic future technology.

Another particular factor here is threat intelligence sharing, and we talked about information sharing. Countries like Israel and Estonia have already formed national security operation centres for each industry so they have situation awareness. If a train network here gets attacked by a foreign state actor because there is cyberwarfare going on, it is very likely that Melbourne, Brisbane and the other capital cities will be attacked as well. Bringing up, centralising and sharing information so that everybody has situational awareness both at an individual organisation level and a State or Federal government level will be critically important, and is not well done at this time. Although I must say we do see that happening in the Transport cluster. For example, you are starting to aggregate visibility, but we have a long way to go. The third thing is that we need to clarify the legal and statutory norm for lawful countermeasures so that when a cyber attack occurs we know our degrees of freedom and how can we respond. I will hand to Ms Leggat, who is a specialist in this area, to speak further on that.

Ms LEGGAT: Thank you, Mr Cox. Thank you members of the Committee. Ladies and gentlemen, there is already sufficient law internationally, at common law and in Australia at a Federal and State level to recognise and facilitate lawful active cyber defence. The complexity of the Australian regulatory regime, however, is largely the result of federalism, which means that it is difficult to understand and to apply correctly to the physical, and logical facts of a cyber attack, specifically in relation to electronic law and the lack of uniformity across States and Territories. This, together with the Australian preference for specific and detailed provisions driven by compliance, results in uncertainty and, therefore, a failure to act which, in turn, makes Australia an attractive target for malicious actors.

There are literally hundreds of statutes that deal with issues relevant to cyber active defence. But those most relevant fall into a body of surveillance law and surveillance versus privacy—the Privacy Act, the Telecommunications Act, the Telecommunications (Interception and Access) Act and the Surveillance Devices Act—and we also have the Criminal Code Act. Those laws generally include prohibition against surveillance, interception and access but they also provide for exceptions. Generally, what we are looking at is, is there a use of listening, optical tracking and other kinds of devices on a network? The Criminal Code Act provides specifically for very defined offences. They include physical and fault elements, each of which needs to be proven before there is a chance to find somebody guilty of an offence. The Criminal Code Act also provides for self-defence. But, once again, it is difficult to thread all of the requirements together to find out what a person can properly do and we end up stagnant and not responding.

The active of cyber defence response that we seek in terms of the submission is that we ask you to simplify existing legal complexity to provide the certainty needed to ease the adoption of the active cyber defence and better protect the digital and critical infrastructure of not only New South Wales but also Australia more broadly. To confirm in at this point a specific example of how you can do that, how you can provide clarity, I want to ask that we possibly discuss the issue of self-defence in the Criminal Code Act, because it recognises self-defence of a person or property against any unlawful interference, loss, damage, destruction and even to the extent of trespass and removing somebody from what is premises or land and property. In my view there is a capability to interpret this as an application into cyberspace in the same way that we have seen international conventions such as the Cyber Crime Convention under the Council of Europe Convention which really translated trespass and property law into unauthorised access. It is this kind of clarity that we seek. Thank you.

The CHAIR: Can you provide more information on or examples of what you mean by active cyber defence?

Mr COX: Absolutely. I am not exactly sure how much familiarity you have with the space but in cyber intelligence it is possible to know a lot about what is going on the dark web, in the deep web, on social media without having to break passwords or to break any law because it is notionally in the public domain. There is a domain called Open Source Intelligence. It is a well established domain globally but not very well understood or adopted in the Australian non-security sector. To give you an example of an active cyber defence measure, some of our clients would seed their data bases with fake information, fake records—we call them honey records—which, if they were stolen, would be identifiable when you analyse the data.

We would have a surveillance service, somebody that is trawling the dark web for information that is available for sale. If they identify this fingerprint, they would be able to say "Wow, you have had information stolen. What is more, we can tell you that it is from this data list". So it is from this particular database from that time period, or this particular backup. You would have then a very good sense of what information was stolen. We have all heard the words "there is no evidence of any data having been taken". I usually refer to them as weasel words because that does not give me any comfort at all. So this is actually providing assurance or a measure of assurance as to the fact that I may, in fact, have lost information. That is one example.

Mr DAVID SHOEBRIDGE: Have you got that graphic on page 14 of your submission that I found really helpful? It took us through the active defence, you call it the grey zone.

Mr COX: Yes, the uncomfortable.

Mr DAVID SHOEBRIDGE: I found that very useful to work through.

Mr COX: It is the uncomfortable grey zone between passive defence which is what we are doing at the moment which is basically trying to build walls to stop the bad guys getting in and hoping that the walls are going to hold which are continuously circumvented. Now you do need fire walls and you do need cyber hygiene and the Essential Eight as proposed by the Federal Government are important measures to provide defence ability. But the problem is that you are trying to climb a curve of perfection which gets increasingly expensive the further you go up it. Most organisations are way down here at the very low level. So you do need to invest in those things but by itself, we are talking about that blind boxer metaphor. No military can defend against every threat. They invest in intelligence and understanding the intentions and the capabilities of their adversaries and then they defend against the threats that they consider to be sufficient risk to justify the investment.

The Hon. ADAM SEARLE: What is a botnet take down in your grey zone?

Mr COX: For example, Microsoft took down the trickbot network recently which is a massive bot network which was used to mount all kinds of ransom ware attacks. They were controlling computers that compromised that people do not even know, they were using those computers to mount massive attacks, similar to the one that occurred to the Victorian Government health sector a year ago when they shutdown the hospital IT systems for a month. Microsoft has moved to force that infrastructure to go off line. In fact, there was an article just this week about that particular network that it has proved to be unsustainable. The trickbot guys are trying to get themselves back up again but they have actually suppressed them as a—

The Hon. ADAM SEARLE: So that is an example of an activity that you think government should licence some affiliates to be able to undertake to dissuade mal actors?

Mr COX: That is a lawful countermeasure which Microsoft has no doubt undertaken in conjunction with, first of all, the FBI and I will be able to table on notice an article about this which talks about some of the other jurisdictions around the world which they have been able to collaborate with to take it down.

The Hon. ADAM SEARLE: Ms Leggat, do you have something to say about that?

Ms LEGGAT: I want to add to that. Microsoft has done a lot of really good defence and active defence work over the years. What is interesting and important about the trickbot takedown is that they actually applied to court for an injunction. That injunction was based on nine different pieces of legislation. What we are asking for is more than that. There will always be a time when you have the luxury of time to go to court and say, "Please, can you make this act lawful?" But active cyber defence needs to respond more automatically. We need clarity before. There is not the luxury of time if you are under attack.

A legality and the liability that attaches to the action is dependent on whether you respond before, during or after an attack. If you respond afterwards, and that is moving to the right hand side of the diagram that you have, you are more and more likely to need the involvement of law enforcement because it is more dramatic. If you are under threat and it is happening right now we need clarity that you can defend yourself; that you can do a take down action and that is where self-defence becomes so powerful. Because frankly, you would be negligent if you do nothing and just watch someone infiltrate data at a health centre.

Mr DAVID SHOEBRIDGE: That is where the legal grey area is at the moment? Maybe it is not legally grey, maybe it is actually legally clear because what you would be doing in that situation where you are aware of a threat, the threat is imminent and instead of waiting for it to happen you actively go out and disable that threat. Does that place an organisation at legal peril because they have gone out and caused damage to a system?

Ms LEGGAT: In the law of self-defence there is an enormous body of precedent that provides for what is lawful in terms of a pre-eminent action, action during an attack and action after an attack. What we are asking for, I am specifically asking for in terms of interpretation of existing law, national law to cyber space, does the principle of self-defence apply to cyberspace and networks in the same way that it does to property and to land?

The Hon. ADAM SEARLE: Ms Leggat, would you be able to provide to us on notice some further detail around that submission? Some more material that we could have a look at about that body of precedent to which you have referred?

Ms LEGGAT: For this hearing, with pleasure.

Mr DAVID SHOEBRIDGE: The concept of self-defence from property actually causing damage to another to protect property is much more complex than kind of reasonable force to protect an individual's personal integrity, is it not? It is actually much more complex and thankfully much more constrained?

Ms LEGGAT: It is complex but there again there is an enormous body of what is acceptable and lawful and not. Even our Criminal Code Act actually specifies that you can cause damage to property but you cannot cause injury and death. It is very specific. So if you have a cyberattack in order to defend against that you are going to, let us say, de-activate an air conditioning system that has malware in it that is coming into banking system, and you take that against what sort of damage may result if you do that, then you might go down with damages to the owner of the building. Maybe you own the building. That is very different from if you have got malware coming out of connected vehicles and if you take those down you then cause injury and death. But this is exactly the point. We are trying to establish in terms of reasonable norms of behaviour in cyberspace does the law of self-defence apply? If so, how?

Australian law if so specific. There are many different examples in terms of other laws. The Telecommunications (Interception and Access) Act specifically allows for network protection duties and the people responsible for those functions much more power than organisations generally have. Those kind of powers link back to the Telecommunications Act and to ASIO and other Acts. Most of what we are dealing with, the prevention against surveillance really deals with law enforcement activity. We need to make a distinction between what is properly law enforcement and law what is okay and necessary for an organisation or a State Government to actually do in order to defend itself.

Mr DAVID SHOEBRIDGE: Are you saying that there is a need for State and Federal laws to expressly authorise that kind of self-defence and put some boundaries and standards around it? Is that implicit in your submission?

Ms LEGGAT: I would very much like to see that. I do not understand why the principles, of the law of self-defence, in tort law, criminal law and internationally in common law across every single ambit. But we steadfastly refuse to say that it applies to our networks even when the criminal code says that you can remove somebody from a premises or facilities.

The Hon. ADAM SEARLE: Given that a number of these mal actors are foreign states, or people acting outside of New South Wales, is there some issue with the New South Wales Parliament reporting to enact that kind of self-defence regime? Or is that something that should more properly be dealt with at a national level? Or is there room for both the State and the Commonwealth to act independently but in a supporting way.

Ms LEGGAT: National security is a national issue under the legislative powers of Parliament that fall under section 51. It is also bipartisan. It should be dealt with everywhere in the same way as air services, where everything that relates to the security of Australia is dealt with at a Federal level. But similarly, the Telecommunications (Interception and Access) (New South Wales) Act actually includes provisions to recognise agencies falling under the provisions of the Federal Trades Recognition Australia. You can add whatever detail, but it would certainly be compelling if you were to motivate this thinking at a Federal level.

The Hon. ADAM SEARLE: So there is space for New South Wales to act on this, in your view?

Ms LEGGAT: Yes.

Mr DAVID SHOEBRIDGE: This active defence seems, from my reading of it, really expensive. Am I missing something?

Mr COX: Thank you, that is a really good question. The fact is it is far less expensive. The problem is that when we are taking a passive measure, we are trying to fix every vulnerability and block everything that should not be allowed, and you are never going to succeed in doing that. There are always ways of circumventing it, because the technology moves on.

Mr DAVID SHOEBRIDGE: It is a kind of Maginot Line.

Mr COX: Yes, exactly. The measure we did not get onto was deception. Technologies are available now to create what are called honey pots, which are basically fake computers that look like real computers. What you find is it is possible to lay these in any network, not cheaply but quite inexpensively, and have them let you know if there is a malicious actor moving around in the your network, because they will detect their activity. The beautiful thing about that is that unlike the—the statistic that I did not quote from the Ponemon Institute is that the average organisation is getting tens of thousands of alerts per week. There are just not enough humans to analyse all of those alerts, because the problem is there are so many false positives. Eighty per cent of the alerts they get in these security operation centres are false.

Mr DAVID SHOEBRIDGE: It sounds like a drug dog operation.

Mr COX: But when you use deception tools, they only produce true positives. When somebody touches your honey pot, you know what computer they are coming from. If they are trying to upload malware to your device—to your decoy—you know what their toolkit is. Even if it is malware that has never been seen before—if it is what they call a zero-day attack—you get a code sample of something that you know is malicious, because they should not be messing with this machine. In fact, these are the tools that are used by Federal agencies to defend the country.

Mr DAVID SHOEBRIDGE: Is that a space that small and medium-sized enterprises could operate in?

Mr COX: The alliance right now is working with a relatively small Western Australian water organisation to deploy a set of tools as a proof of concept in partnership with some of our members, including Telstra and some Australian sovereign deception technology manufacturers. I would envisage that the ongoing service, should they determine to adopt it—they are writing it up as a case study—would be well within their financial capacity to obtain and keep.

Mr DAVID SHOEBRIDGE: Is the role for a provincial government like New South Wales an educatory role? We have spoken about some of the regulatory space, but in this area is it an educatory role? Is it a standards-setting role? Is it providing resources to small and medium-sized enterprises? What is the role for the State Government?

Mr COX: Actually you as a State Government, and certainly the critical infrastructure for which you are responsible, is urgently in need of these measures so that you can defend yourself in the first place.

Mr DAVID SHOEBRIDGE: That is the starting point?

Mr COX: That is the starting point. The issue is that most organisations do not have a big budget to try what seems to them to be exotic new technology. What we have found is most organisations have a budget for running annual cyber drills. So, as an alliance, a bunch of are putting together quite a bit of pro bono consulting resource and engaging with a number of State government agencies. We have some engagement with New South Wales—which I would prefer to detail on notice—as well as Queensland, Victorian and Western Australian government agencies, and Federal agencies.

We are exploring this with a view that incorporating some of these tools, like deception and intelligence, into their annual cyber drills would give them the opportunity to assess the real value. We believe that they will find that there is compelling value found by going down this road, because you tip the balance of power against the enemy. The enemy can pick you off any time they want, but now their adversary has to be careful because any false step could be a honey pot. So it actually changes the balance of power and starts to exact against and accost your adversary. They cannot get off scot-free now.

Mr DAVID SHOEBRIDGE: But to change that risk scenario, my understanding of your submission is that you would need a honey pot or similar to identify where the threat is?

Mr COX: Yes.

Mr DAVID SHOEBRIDGE: But you also need to be carrying a big stick, where you can actually give them a whack and take them down.

Mr COX: Which is Ms Leggat's proposition about—

Mr DAVID SHOEBRIDGE: Those two things work together, is that your position?

Mr COX: We classify active cyber defence as cyber intelligence, cyber deception, active threat hunting and lawful countermeasures.

The CHAIR: If you are able to provide on notice any of the work that you are doing with any State government agencies, as you just mentioned, that would be really helpful.

(The witnesses withdrew.)

(Luncheon adjournment)

RUPERT TAYLOR-PRICE, Chief Executive Officer, Vault Cloud, affirmed and examined

JOHN FRISKEN, Director Professional Services, ISG Consulting Pty Ltd, sworn and examined

MILTON BAAR, Director Cyber Security, ISG Consulting Pty Ltd, affirmed and examined

The CHAIR: Welcome back to everyone who is tuning into our broadcast of this inquiry today and welcome to our witnesses that are joining us for the session this afternoon. You are entitled to make an opening statement if you would like.

Mr TAYLOR-PRICE: I have two tenets to my opening statement. One is around citizens' trust and the other one is around harmonisation. Citizens' trust in government is absolutely critical for the operation of government to succeed. We need citizens as much as they need us. You can see that in what happened, for instance, in e-health. In e-health the survey results show that there was a lack of confidence in privacy, security and sovereignty. That resulted in many hundreds of thousands of people opting out. There is also research that shows that people that opt out of that system have worse health outcomes, including death, so people are literally willing to sacrifice their quality of life and health outcomes in exchange for privacy. In that particular case, they did not decide to believe that government was trustworthy of holding their data. It is a pretty strong statement when citizens are willing to go that far.

We also saw a lot of controversy especially in the media, and social media and letters, around the COVIDSafe app being hosted on a foreign and offshore cloud provider. Of course, the economic impacts of being unable to trace COVID-19 are pretty obvious for us all. That is backed up by some work done by the Information Commissioner where they found that 93 per cent of people expect sovereignty of their information when dealing with organisations in government, so there are clear citizen expectations there. If you think about cybersecurity as the fifth domain of warfare, it is a very important capability for us to have.

Today we are very much a consumer of services. I would say that we are not pulling our fair weight as a Five Eyes partner. We are not contributing to that technology, we are not contributing sufficiently to that capability and we would need to improve there. That comes more into the citizen realm when you think about the effects of COVID around our ability to manufacture things like personal protective equipment and other things. It has woken us up to the fact that we actually need certain capabilities here domestically, particularly in the technology and cybersecurity space.

Skills, education, training and competency are all important, but we also need to build capacity within our government and within our private sector and government supply chains. Are we sufficiently protecting our digital borders? Are we successfully protecting our citizens' data and privacy? Are we living up to the expectations that citizens have on government? I would state that is different to the expectations that they have on the commercial sector. A lot of people say that citizens hand their data to large companies like Facebook and others and therefore they have no regard for their privacy. I think that is a flawed argument, and certainly the expectations that citizens have of government are very different to those of commercial organisations.

The second point that I wanted to make was around harmonisation. The organisation that I represent works heavily in the Federal Government and also works within the New South Wales Government. We have found that there are vastly different standards and expectations between Federal and State Government. I would say that the Federal Government is further along the maturity process, partly because they have much more of a national security mandate than the New South Wales Government. That has driven a lot of expertise and maturity in the space. To give you some examples of that, the New South Wales Government has a data centre called GovDC. That is not built to a Federal Government standard called a Security Construction and Equipment Committee zone, which means that we are unable to store Federal Government data in a New South Wales Government facility. You can imagine how that breaks up systems, increases cost and lowers security, and what comes from that.

The way that we handle data classification is different. It is not harmonised between the State governments and Federal Government. Security clearances are not the same. New South Wales Government employees that do not have Federal Government security clearances cannot access, for example, some of our systems that are designed for higher classification environments. You literally have a customer wanting to access a secure environment and not being allowed access that environment because they lack those security clearances. Over all, that disparity between Federal and State Government results in a suboptimal outcome for the country and for all involved. It vulcanises the systems and the data across government, makes it harder to interoperate between different parts of government and is a detriment for all of us. Again, not only is that interoperability a problem but it also results in lower security for the country. I feel that is something that we need to move forwards on. Thank you.

Mr FRISKEN: Mr Baar and myself have put together a statement that we have submitted and it probably says most of the things that we wanted to say. I just want to make a few short comments. We do not think the problems that are being experienced at the moment are related to a lack of standards. We have had experience with a lot of secure agencies and a lot of big agencies. We think the main problem is that those standards are not being implemented. There are a couple of reasons for that. One is really the devolution of security back into the agencies. There was a stronger presence when we started this process back in 2001. Security in a sense has lost its way. In fact, there has probably been an over-focus on policy. There are now about three or four different policies related to cybersecurity in New South Wales. It is a very confusing situation. In some of the major agencies, we have found that in fact they conflict with each other and cannot all be implemented. That is one of the main issues that we are seeing.

The other issue has to do with the emerging interaction of operational technology, information technology and the Internet of Things. The security histories of these three areas are quite different but due to the changing technology, a lot of organisations are being forced to manage it in the same way. There is a high convergence, a lot of which is to do with the internet. What we are seeing happening is that there are essentially different people in the organisation who have responsibility for these. A lot of organisations are having a lot of trouble with actually establishing common standards across these areas and adopting a single governance system. We are seeing that this is leading to a lot of political problems with actually implementing secure solutions within government departments. I could say a lot more but they are the highlights that I would like to bring to you. Is there anything else that you wanted to highlight, Mr Baar?

Mr BAAR: No, I think hearing from one of us is probably adequate at this point.

The CHAIR: The key theme between both of you is this lack of harmonisation. I guess this question can go to you both, with different perspectives. Your argument is that the national system is better—for obvious reasons of national security and all the rest of it—and that rather than have New South Wales implement its own policies it should work with what is happening federally. The fact that we are not doing that here is clearly a risk in terms of data, but is it a national security risk?

Mr TAYLOR-PRICE: I would say yes. I think that most State governments would leave it to the Federal Government to look after matters of national security but the truth is that the world has evolved with ubiquitous data and systems. The threats impacting operational technology and other technologies are now across government and across systems that impact people in their everyday lives. Yes, I think there is a greater existential risk now within the State Government that is a matter of national security.

Mr FRISKEN: I would make the comment there that back in say 2005 New South Wales led the country in information security. In 2008 we were involved with the update of ACSI 33, which was the national standard at that stage, and we moved it into the information security manual, which is the one that is currently in force. As part of that I introduced a lot of what we were doing in New South Wales associated with ISO 27001. They adopted that and at that point started to change the way that they were implementing security from a purely technical approach to security, which it was to them, which was not really very satisfactory, to a more risk-based approach based around ISO 27001. Ultimately, it is probably correct that at this point in time that they would lead New South Wales and that is partly because we have dropped the ball. We had a very good start and had not followed through. We established a lot of policy and that policy was embedded in the agencies but the agencies do not follow it. That is the main problem. I think the national government now leads New South Wales but it is good to note that we led the national government 15 years ago.

The Hon. TREVOR KHAN: I have to say that evidence is, as best as I can determine, inconsistent with what Ms Price said before lunch. She appeared to me to indicate that it was New South Wales leading with the assistance of the other States and essentially the Federal Government being brought along, it is probably euphemistic to say, kicking and screaming to a result. I am wondering how she paints a positive picture in terms of where things are up to and that is not what you are saying.

Mr FRISKEN: I think at one point in time it certainly was right that New South Wales clearly led the nation in information security.

The Hon. TREVOR KHAN: She is talking about now.

Mr FRISKEN: Yes, I know. I think possibly in some areas of policy New South Wales still has got good policies. The problem I think you will find is that those policies are not implemented within the agencies and they have not been operationalised. It is the practice where things are falling down. I would say that the national government has picked the game up a lot in the last 10 years and from a policy point of view would be pretty much equivalent now. In terms of Mr Taylor-Price's comments about things like data centres, that sort of thing, Mr Baar would know better than me.

Mr BAAR: There are problems with the implementation and it is to do with the potential of the perceived sovereignty of making decisions. State Government's do not like to be directed by the Commonwealth and the Commonwealth is not keen on being steered by the States. If it is determined to be a State only matter then a State Government will typically say we are doing it this way, it suits us. The problem is when you need greater interaction. And anything such as Joint Special Operations Command outside of Canberra, which is potentially looking at a whole of Australia approach to cyber security it cannot interact and operate directly with state-based agencies that do not have the correct level of security process or are compatible. The time to find that out is not when something happens.

The Hon. ADAM SEARLE: Just on that, for example in early 2016 there was a hacking attempt on sensitive mining and resources data held by the New South Wales State Government and as best anyone could tell that was from a foreign state actor. I had some involvement in chasing the State Government up and received a briefing from them, which I found fairly unsatisfactory. The long and short of it is, in the modern era that kind of data, although held by a State government only, could well be of national economic interest if not national security interest, so surely that speaks to the need to have a greater level of coordination between Commonwealth and State governments, would you not agree?

Mr BAAR: It certainly does. For example, the New South Wales State Government's policy for information classification, labelling and handling, which I had a hand in writing, has towards the rear appendix the mechanism for determining what is the actual impact of this information if you lose it, if it is damaged, if it is unavailable. The preferred mechanism used in the appendix is the Commonwealth Government's business impact levels. But, they do not map directly to anything the State Government recognises. Even though we have it within our own information classification, labelling and handling standard there is a great difficulty in trying to operationalise it because all the information New South Wales government departments appear to have is unclassified.

The Hon. ADAM SEARLE: We have had a number of reports from the New South Wales Auditor General, 2018, 2019 and 2020, which makes a pretty compelling case that State agencies and local government are not really prepared to monitor when breaches occur in a timely way. We heard evidence before lunch that the average time period between a breach occurring and an agency becoming aware was 283 days, or something like that. There is a longer period before anyone tells those affected. That is of great concern. In the Anglicare incident I think the best information was taken to somewhere, I think it was New Zealand, and then I think more recently we have had the bomb hoax email that affected HSC students causing great disruption here in New South Wales. Now the Premier is telling us that originated from outside the country. Does New South Wales actually have the right tools to say with authority where these attacks are coming from? Or is it just a best guess based on various indicia?

Mr BAAR: In cybersecurity, in cybercrime, attribution is one of the most difficult things. You can make an assumption but actual attribution, unless someone is actually caught is extremely difficult. The difference between a state-based actor and an interest group potentially of students with reasonable levels of skills is difficult to discern.

The Hon. ADAM SEARLE: Although, nation state actors I have been told by those working in cybersecurity sometimes leave their fingerprints by the type of devices of the type of tools that they have at their disposal which non-state actors do not have, is that not the case?

Mr BAAR: That is very true and it depends on the type of attack and the type of exposure and the environment. I am making a general statement because specificity is what is required.

The Hon. ADAM SEARLE: Given the advent of VPNs and people being able to make it look like they are doing things from outside of New South Wales, how confident can we be that this data has been taken to New Zealand or this email came from over there, is that just a best guess?

Mr BAAR: There are generalised answers but it really depends on each specific situation. As you indicated, if they leave traces, if they leave fingerprints and it can be determined that those traces and fingerprints are not decoys then, yes, there is a reasonable likelihood of being able to make an attribution of a trail or an actor. But, that is just a very general statement.

Mr TAYLOR-PRICE: If you look at general crimes, there is an error rate in attributing the perpetrator of any crime. It is particularly difficult in cybersecurity. It is particularly easy to place evidence that misleads people. When I hear of someone or some country being attributed for a certain action, I would certainly say that my confidence in what I hear is generally low, knowing that it is very hard to conclusively attribute actions like that.

The Hon. ADAM SEARLE: Leaving aside that certain tools are not generally available to non-state actors though, depending on the kind of attack?

Mr TAYLOR-PRICE: Anything is available at the right price.

The Hon. ADAM SEARLE: That is comforting.

The Hon. TREVOR KHAN: It is a bit of a mistake to describe this as state and non-state actors. There is a gradient of involvement by the State in some of these. Some of the Russian organisations appear to be linked to the intelligence agencies but seem to operate outside what you would have considered the normal government enterprises. Is that not right? They seem to have identified quasi private enterprises.

The Hon. ADAM SEARLE: Contractors.

The Hon. TREVOR KHAN: Yes.

The Hon. ADAM SEARLE: Outsourcing.

Mr BAAR: Yes, hacking for hire. I think the issue of attribution is interesting, but I think that for the New South Wales Government the issue is more about detection and prevention, and potentially mitigation. It really possibly does not matter who does it.

The Hon. ADAM SEARLE: I think Mr Frisken was saying that there are policies in place but they are not necessarily being followed. We have had submissions and evidence in favour of a strong cybersecurity agency that sets the standards but also audits agencies with line responsibility to make sure they are actually being followed. Would that seem like a sensible development to you?

Mr FRISKEN: I think that would be a situation that would be better than where we are at the moment. I would think the ideal situation would be what was originally implemented but then was dismantled. That was where there were policies that were dictated, like standards, and then there was independent certification of agencies following that. The problem with having a central agency doing it is that you are not going to have as much confidence as if it was an independent organisation.

The Hon. ADAM SEARLE: You mean the certification?

Mr FRISKEN: Certification, because there is always—

The Hon. ADAM SEARLE: Who should do the certification?

Mr FRISKEN: Yes, I would think that would be a higher standard than having a central agency.

The Hon. TREVOR KHAN: But who?

Mr BAAR: An external objective entity that is not part of the creation or the implementation of those standards. Sarbanes-Oxley was introduced specifically to stop that type of behaviour in the United States. We have the legislative framework that exists right now to say, for example, a government agency could be set up to provide preferred frameworks, preferred standards, and a separate arm of Government could audit how that has actually occurred.

The Hon. ADAM SEARLE: Mr Khan just posited that the Auditor-General of New South Wales could fulfil that audit function.

Mr BAAR: Yes, the Auditor-General could certainly do the auditing, but they should not be the agency that sets the standard or oversees the implementation of it. It should be a completely separate audit function. I think that would be a much better governance structure.

The Hon. ADAM SEARLE: Underpinning that we have heard evidence in favour of a mandatory disclosure regime like there is in the Commonwealth and also data sovereignty, that at least some sensitivity dataset should be kept onshore, and Mr Khan, in fairness, has raised the issue about accessibility. Does that mean that certain datasets should only be able to be accessed onshore as well?

Mr FRISKEN: Mr Taylor-Price is perhaps better to comment on it, but Parliament in New South Wales has just introduced the policy of public cloud by default, which basically means that from a procurement point of view the baseline for procurement is going to be public cloud. Making that sort of thing is going to become very difficult.

The Hon. ADAM SEARLE: What does that actually mean?

Mr FRISKEN: At the moment the arrangement would be that agencies would, from a cloud point of view, be using GovDC, which is like a private cloud provider. Making a public cloud provider as a default would mean that you could open up all sorts of other private organisations who are providing hosting of applications or hosting of rack space to government agencies, so creating a more competitive environment, I suppose, from a procurement point of view. I think that is correct, is it not?

Mr TAYLOR-PRICE: Yes.

Mr BAAR: The issue is the risk based trade-off which is sometimes being made heuristically. There is no thought that goes into it. It is an economic driver that says we should go for the least expensive option and that will be opening it without necessarily a quantification of loss.

The CHAIR: We are doing that now, but if we were to properly think about that, as this Committee is trying to do, how easy is it to address these things? If they are not properly thought through and we are just saying we need to put these things into whatever cloud that government agencies are using, how easy is it to fix those problems in the future if we do not deal with them properly before that?

Mr TAYLOR-PRICE: Could I actually go back a few questions and add to some of them?

The Hon. TREVOR KHAN: Yes.

Mr TAYLOR-PRICE: On the certification discussion, I absolutely agree there needs to be independent certification. The reality is today that my organisation is an unregulated organisation. I am effectively making decisions of national security and I do not carry the consequences of those decisions—and not just national security, citizen trust, the operation of Government and those things. I do not think it is appropriate that the level of power that I, or especially a multinational organisation, should have over the sovereignty and the future of this nation.

That brings me on to regulation or a regulator. If you think about the banking sector, what we do as the cloud industry and cybersecurity is far more important and impactful than the banking sector, yet look at the regulations and the regulatory power that exists in the banking sector. And we are unregulated. I struggle with that every day, that something so critical to the operation of society can not just have a weak regulator but really be in the absence of a regulator. Those decisions are being left to commercial organisations like mine, which of course I am very happy to make, but just from a nationalistic perspective I do not think that is the right answer.

The CHAIR: How are we here? I know you want to talk about some other questions that we have asked, but how is this the situation?

Mr TAYLOR-PRICE: Because we are an emerging industry. I imagine when the banking sector started it was probably unregulated as well—

The Hon. TREVOR KHAN: Not probably; it was.

Mr TAYLOR-PRICE: And, of course, you get perverse outcomes when you have a lack of governance and regulation, you have people making commercial decisions with people not thinking about the outcomes of the country.

The Hon. ADAM SEARLE: Can you tease that out a little bit as to how this is unfolding and what the practical impacts of this are?

Mr TAYLOR-PRICE: We have some guiding principles, as mentioned—

The Hon. ADAM SEARLE: As a private corporation?

Mr TAYLOR-PRICE: Yes, as a private corporation, so we hold sensitive government data and systems for various governments in Australia, so we have some guiding principles such as ISO 27001, the Information Security Manual and the Protective Security Policy Framework. In reality today, we decide which of those we implement and how we implement them. We do have some auditing, but we choose our auditor and we pay our auditor. We can shop for the auditor that we want.

The Hon. ADAM SEARLE: The Government does not set the standards you have to meet and does not impose any audit requirements?

Mr TAYLOR-PRICE: They set the guidelines that we should work towards, but there is no regulator that then will look specifically at our compliance with those standards and question the decisions that we have made.

The Hon. ADAM SEARLE: Are you required to keep this sensitive data onshore?

Mr TAYLOR-PRICE: We do. That is something that we specialise in.

The Hon. ADAM SEARLE: Sure, but is it something that you are required to do?

Mr TAYLOR-PRICE: No.

The Hon. ADAM SEARLE: You could have made a commercial decision to keep it offshore, for instance?

Mr TAYLOR-PRICE: Correct, so to talk about sovereignty, which was one of the latter questions, there are three forms of sovereignty for me. There is physical sovereignty, which is the data in the country, and I think that is the one people talk about a lot but is actually not the most complex. You have operational sovereignty, so if your data is onshore but everyone managing it is offshore, there is clearly a risk to that too, and I am actually more worried about who is looking at the data than whatever the data is that they are looking at. Then you have legal sovereignty, which also comes into jurisdictions, so if your data is hosted by a foreign company or hosted offshore, you could or would be subject to other legal jurisdictions.

People can make an assessment today on what those laws in those other countries are and if we are comfortable with accepting the risks around that; however, we cannot control their governments and their parliaments for their future legislation that they make. The idea that we could just switch off the use of some of these systems and bring it all back and control it is unrealistic. It is a bit like COVID-19, we could not make all the things that we wanted to when we wanted them. It would take absolutely years to restructure systems around that. Those are existential risks that no-one seems to own within Federal or State government. They are not things on people's minds on a daily basis. I think COVID has changed that, but historically we have not seen that bit of focus.

The Hon. ADAM SEARLE: Does there need to be an independent regulator doing this? If so, who should that be?

Mr TAYLOR-PRICE: If you wanted a national one it could come out of the Department of Home Affairs. Given the scale and the complexity of the sector, it probably needs an Act of Parliament that legislates a new, independent legislator that has some power to make some decisions and decide what is best for the future of the country.

The Hon. TREVOR KHAN: It really has to be at a Federal level, does it not? You have corporations that operate well and truly beyond State borders and health systems that deal with people from multiple States. Otherwise it is like the old railways—we will end up with different gauges in different States.

Mr TAYLOR-PRICE: I agree with that completely. But it still needs to happen.

The Hon. TREVOR KHAN: I am not arguing the toss on that. It just seems to me that if you try to do it at a State level then you will create significant costs for various of the actors in complying with different State jurisdictions.

Mr TAYLOR-PRICE: Correct.

Mr BAAR: There was an earlier comment about harmonisation and this is where the harmonisation is important. It can be done and there are frameworks that exist between the Australian National Audit Office or attorneys-general at a State level. There is a capability right now, but there are other issues of implementation and it does not come free.

The CHAIR: Yes, and issues of implementation. At least the Federal Government is looking at this in some way, but it is extraordinary to hear that we have gone backwards over 20 years when technology has improved.

The Hon. TREVOR KHAN: Again, I will say that that is not consistent with the evidence we heard before lunch.

The CHAIR: I am entitled to test the evidence that is before me now and I am really interested in it. To hear that we have gone significantly backwards in 20 years or since 2001 when this started, or in 2005, is extraordinary to me, when we are moving more and more things online and putting ourselves at more risk during that time. I cannot understand why it is not more of a front-of-mind issue for the State Government. Based on that, it seems extraordinary that all we have is a little bit of a cyber something in the customer service department somewhere. Clearly we need to resource this better. We heard some evidence this morning that, essentially, this is dealt with inside each agency and, even then, it is not in some agencies. Some agencies within government will have a policy that you are saying is not even followed and then some agencies do not have a policy at all. That is extraordinary.

Mr BAAR: It depends on the type of agency. Large agencies such as transport, which has become an amalgamation of the other types of agencies, inherited multiple schemes and systems generally based on 27001, but not always, and the process of attempting to aggregate this into a single entity has, over time, been met with a level of pushback. Even though a secretary might say, "This is what I wish to occur", the operational, older entities within that superagency are not necessarily keen to do it or they want to do it a different way. For example, trains may want to do it a different way from buses and, even though it is the same type of information being managed in the same type of way with exactly the same type of outcome, if it becomes exposed there are differences at an operational level.

The CHAIR: That may be so but would you not argue that this should not necessarily be able to be dealt with on an ad hoc basis by a department? I am not completely aware of the details of this but there is a department that is currently tracking movements our movements around the State using different points of our data. I think it was implemented in terms of COVID but I do not know. How can it be possible that we do not have all of the information about that and that it is decided on an ad hoc basis within a department?

The follow-up question is: Who should ultimately be responsible? An independent regulator? Even within a department if there are policies—first of all, there should be policies and in some there are not—they should be followed. Those are the basics. How should we deal with this across government to make sure that, at least in the New South Wales Government, we are being a bit more consistent about it? We need an independent regulator to certify those things. What would be your suggestion to deal with this across all of government to make sure that we have some basic consistency and information about what is happening with our own data?

Mr FRISKEN: One of the issues I think that should be addressed first is that there is a lot of policy confusion at the moment. We had a situation back in 2006/2007 when we had a single policy, which is 27001 and the control sits beneath that. That was fairly clear, and then we had certification. Since then we have introduced in New South Wales at least two other frameworks that are potentially incompatible, which are the ASD Essential Eight and NIST, which is a US standard. Both of those are good but I do not see the point. They are different approaches for doing the same thing. Most standards—almost 100 per cent of standards—that are adopted by government agencies, apart from cybersecurity, are European; they are based on ISO and take a certain approach to how that is implemented using similar systems.

In cybersecurity we introduced a completely different set, so you have an organisation that is saying that you have to implement NIST because it is a new framework but we have 27001 as well. How do you think an individual agency is going to react to that? They have no idea. What should we do? Then we have the complex agencies that are running operating technology—industrial automation—with another set of standards, 62443, which is another ISO standard that is different again. We have this really complicated approach at a policy level. That is probably one of the reasons why there is nothing happening in terms of implementation, because most government departments probably have no idea how to meet that. I would think that is one of the things that needs to be sorted out pretty quickly, to try to simplify that, and get back to a set of standards and policies that can be simply certified against at the moment.

Mr TAYLOR-PRICE: Every one of those decisions goes off track from harmonising nationally.

Mr FRISKEN: Yes.

Mr DAVID SHOEBRIDGE: I was digitally tracking you on the web feed upstairs. We had some evidence earlier today from Professor Varadharajan from the University of Newcastle. He said that simply adopting those standards—whether it is ISO 27001—for security management system accreditation or the like is not necessarily the end point because it is very static and not necessarily well crafted for the different roles that government undertakes. For example, you might have a bespoke thing for health, a different thing for transport and a different thing for policing.

Therefore, his proposition was that the State Government should take a leadership role and come up with some statements and protocols that are publicly disseminated that cover those different types of agencies or government work. They would have reference to the standards but be living documents. I am not describing his evidence particularly well, but I think that is the thrust of that evidence.

Mr BAAR: I would respectively disagree with Professor Varadharajan. We have worked together at Macquarie University and other places. The 27001 is not static, it is a cyclic process. It is a plan, do, check, act model that you continue forever. It is not an end point. I am one of the Australian authors of the standard, having starting work on it in 1988. It took 12 years to become an international standard published.

The Hon. ADAM SEARLE: It is a process, not a fixed point.

Mr BAAR: It is a process and it follows something called the Deming cycle. You are literally a hamster on a wheel going around for ever because you never reach the end; you are constantly improving and identifying deficiencies and improving slowly as you go along.

Mr DAVID SHOEBRIDGE: You say 27001 but, as I understand it, and I could be wrong, there are a series of smaller policies under it that deal with cloud and information technology.

Mr BAAR: Sort of. That is a reasonable characterisation. There is the 27000 suite of standards and 27001 is the only standard to which you can be internationally certified. If you are certified to 27001 in Australia it is recognised anywhere in the world. It is an information security management standard. Then there are things such as 27002, which is a checklist such as you should do this et cetera. All of the others are checklists or guidelines but you cannot be certified to them.

Mr DAVID SHOEBRIDGE: Again I am badly summarising the evidence of Professor Varadharajan but my take away from it was that those standards are very high level and abstract. If you are just going to hand them over to a small or medium enterprise or even a government agency there is a translation problem and it is not going to be implemented and there is a kind of obligation to almost make a kind of ready, adapted manual, if you like, to translate them to government and small and medium enterprises.

Mr TAYLOR-PRICE: I agree with what you are saying. So there is a lot of subjectivity to ISO 27001. We have implemented it as an organisation. You can implement it to a very high standard or you can, sort of tick boxes and get it through. I feel like the standard you are talking about is the Federal Government's protective security policy framework and the information security manual. They are explicit and specific on what you need to do in various components whereas ISO 27001 is more about having the right governance and framework and processes around your business. Those other ones are specific—this encryption standard is installed here to this standard or to this level.

Mr DAVID SHOEBRIDGE: Are you saying the Federal Government is doing some of that more finely grained–

Mr TAYLOR-PRICE: Correct.

Mr DAVID SHOEBRIDGE: And it is an off-the-shelf solution that we can apply in New South Wales?

Mr BAAR: The Federal Government standard is proscriptive whereas I say 27001 states that every organisation should adapt it and implement it to suit their specific requirements, which is why every State Government entity could implement 27001 differently from each other to meet their specific needs. Protective Security Policy Framework [PSPF] and ISM are very proscriptive: you will use this, you will use this, you will use this and 27001 is a better fit for diverse government agencies.

Mr FRISKEN: You could arguably implement ISO 27001 as a process. I think it is the most mature process that is out there. It is certainly the only one that you can actually certify. You can then seek out best practice in any number of areas and from a risk-based point of view you can adopt that. That is the beauty of the ISO 27001 standard, you can adapt it to the needs of your organisation and the risks your organisation is facing. I think the ISM is still quite a technical standard. It is good in that it provides advice in relation to certain issues but you could not actually pick it up and say, "Everyone has got to use this." If you did, you probably would have a budget problem. A lot of agencies would not need to go to that level to protect things.

The problem with doing that is that agencies are going to resist that. So you need that oversight to go into an agency and say, "You do need to do something. We need to see it. We need to audit it. We need to make sure that you are taking this seriously." That is what is not happening at the moment. There is no stick there to actually hold agencies accountable.

Mr TAYLOR-PRICE: I would agree. ISM and PSPF are very prescriptive and very difficult standard to meet. There is a cost to that. So the Government has got to make an assessment—and I think the policy it has got in place is appropriate for the Federal Government. You then need to make a decision, is your data needing security less than Federal Government data? If so, which parts of that do you not want to implement? Because there is a cost and a challenge to implement all of those things.

The CHAIR: We really appreciate your attendance today.

Mr FRISKEN: We certainly hope you make some progress here.

(The witnesses withdrew.)

THOMAS COSTA, Assistant Secretary, Unions NSW, affirmed and examined

EL LEVERINGTON, Legal and Industrial Officer, Unions NSW, affirmed and examined

The CHAIR: Do you want to make an opening statement?

Mr COSTA: Yes, I would like to make an opening statement. We appear on behalf of Unions NSW, and we thank the Committee for the opportunity to participate in this inquiry into cybersecurity. As outlined in our submission to the inquiry, Unions NSW is not in the position to provide the kind of specific information and insight requested by the Committee's terms of reference, given the level of detail that is sought in respect of the Government's operations and expenditure and a level of detail that we do not have access to. However, Unions NSW is pleased to share our concerns relating to cybersecurity and data more broadly, particularly when these areas of growing importance impact, threaten, or disadvantage workers.

The primary concern of Unions NSW in respect to cybersecurity and data is to ensure the protection of the personal information of people and behavioural data through robust, well-managed regulation. Primarily we are calling for a cybersecurity strategy which creates and imposes mandatory reporting requirements upon all New South Wales Government agencies in respect of any and all cybersecurity breaches. We would like this to be a strategy that will build resilience and other long-term proactive protection rather than a just-in-time reactive response strategy.

In addition, the union movement continues to call for a workplace data regulatory system built on transparency which not only ensures workers know data is generated by them is being captured and used but how it is being profited from, ensuring any benefit received by the New South Wales Government is equitably shared with its workers. We also believe this system should require the New South Wales Government to educate its employees about the data they create in its life cycle.

The New South Wales Government has the opportunity to set a standard for data protection in Australia and the union movement believes the State will be strengthened by a system which prioritises transparency and has processes in place to learn from every breach experienced. We also believe the value derived from the sale or use of employee data should be reflected and compensated in their salaries and conditions in addition to productivity and efficiency measures.

The Hon. ADAM SEARLE: Mr Costa and Ms Leverington, from your submission it seems that you are very much in favour of what some submissions have called "data sovereignty" that is, where certain sensitive data should be kept on-shore within jurisdiction and perhaps access to that data should also be restricted to being within jurisdiction. Do you have anything further to say about that particular matter?

Mr COSTA: We believe that data should be maintained onshore and in-house. The reason is we believe the considerable risk to data is beyond any weakening of consideration. For example, having data offshore in a jurisdiction where laws and regulations can change over which we have no sovereignty or control opens up not just the Government but the data that is held on employees and members of the community to considerable risk. We know this because there have been considerable breaches of data already, and those breaches have not just been data being held overseas but also data being held here. So we need stronger data protection here, but we also note that it is stronger if it is protected here.

The Hon. ADAM SEARLE: Apart from mandatory notification, what would you have to say about the notion that the implementation of data security across the public sector seems to be uneven. There does not seem to be a single point of responsibility, and some submissions have called for a strong central cybersecurity function that sets the standards that agencies have to adhere to. Other evidence has suggested that the auditing of adherence to that should be done possibly by the Auditor-General. Is that a framework that you would support to ensure greater levels of data security across the whole of the public sector?

Mr COSTA: We agree that there should be a department that should regulate all data across the public sector, and which is responsible for regulating and monitoring breaches but also providing transparency around when those breaches occur. At the moment there is no transparency around when data breaches occur. That means that we just do not know how robust protections are at any given time. Without having an agency that has that as their responsibility by allowing different departments to do things differently, we cannot have any faith that it will be done properly. Ms Leverington might have something to add to that as well.

Ms LEVERINGTON: Absolutely. We think that the current approach to cybersecurity is patchy, for want of a better word, and it is very reactive. What we have been talking about is a mechanism—whether executed by an existing agency or a new one—that sets a minimum standard across government, and maybe even a tripartite committee that can exist in each agency to execute that mechanism as is needed by that agency. We think that there definitely needs to be an across-the-board approach to cybersecurity that is then adapted in the most appropriate way for each individual arm of government.

The Hon. ADAM SEARLE: You make some submissions about how workplace and employee-generated data should be managed and protected, and how any monetary benefits that are being derived from it should be shared with the workforce. You have made similar submissions to the upper House Select Committee on the impact of technological and other change on the future of work and workers in New South Wales, and a number of your affiliates have also made admissions to that inquiry. Is that correct?

Ms LEVERINGTON: Yes.

The Hon. ADAM SEARLE: Are those submissions consistent with what you have said here today?

Ms LEVERINGTON: Yes. We also think that there should be a really strong education piece about the life cycle of data and what benefit is derived by someone's employer during the course of their employment. It is such a new and growing area, and for the most part we do not see that workers have an especially strong understanding of what is happening with this kind of new entity that is being developed through their day-to-day work. We think that that would be a really important element in the development of how we handle data.

The Hon. ADAM SEARLE: It is the case that the workplace surveillance laws that we currently have in New South Wales that govern workers at the moment were essentially designed at a time before the internet really took off, and there is concern that those laws are now not really fit for purpose. Is that a viewpoint that you would share?

Ms LEVERINGTON: Absolutely.

Mr COSTA: They are not fit for purpose for a number of reasons, but the two primary reasons that we are trying to explain in this submission are that firstly, they are not fit for purpose because they are not technologically appropriate anymore and they need to be updated. Secondly, they also do not consider the many uses now for data. Data is no longer used just for surveillance. Data is actually now a commodity and can be sold on an open market. It can be used to improve efficiencies and productivity. This use of data has not been looked at in much detail by many agencies, if any, and we are concerned that the Government is using data in ways that could be profitable but not transparent to the workers from whom it is being gleaned. That is an area that we think needs to be investigated. We would recommend complete transparency around when data is being used in that way. Just like surplus labour is valuable in an employment context, so now is surplus behavioural data. That is something that workers generate and deserve to be compensated for.

The CHAIR: Would it be fair to say that there are also not clear lines between the data that is captured from people's working lives compared to their personal lives? Would you say that there should be some clearer distinctions around that?

Mr COSTA: Yes, that is absolutely correct. This year has shown that to us in spades as people have moved to working from home. There would be metadata on when people log into their computers and when they check their emails. There is considerable data about how people now operate their personal lives that could be captured by the Government. We do not know, we have not got access to that. We would like to know and we think that workers deserve to know. So, yes, that is a very important point.

Mr DAVID SHOEBRIDGE: But if you want data security in a workplace, the best way of avoiding data getting into the wrong hands is not needlessly collecting data, or actively going out and searching for intrusive data in a workplace. That is probably one of the best protections, is it not?

Mr COSTA: That would be the best protection. At this point in time, we want transparency so that we know what data is being collected and then we could make a submission about that. But yes, I agree with your position.

Mr DAVID SHOEBRIDGE: And in a workplace surveillance context, some of the data that we know is being captured in some workplaces includes how much time people are in front of their screen, and regular camera shots are taken to assess the period of time people are in front of a screen or not in front of a screen. There should be clear rules regulating capturing that kind of data in the workplace, do you agree?

Ms LEVERINGTON: Yes, absolutely. The Workplace Surveillance Act at the moment does not extend that far. It does not acknowledge the secondary uses of a lot of the surveillance that does take place. Whilst notionally there are various things in place in all sorts of workplaces for security purposes, we see all the time from affiliates from almost every industry the secondary uses of various workplace surveillance, and a lot of the time it is to do with discipline.

The Hon. TREVOR KHAN: Could you give some examples of that? I can think of some with regards to vehicle movements.

Ms LEVERINGTON: Yes, vehicle movements is a great one. We recently saw one go wrong where there was a disciplinary matter. One of the elements raised by this particular government agency was that an employee was in this suburb and the car just moved here and there around the block. The guy went back through his diary and his work-provided car had been in for a service that day.

The Hon. TREVOR KHAN: That is a blunder.

Ms LEVERINGTON: It is a blunder, of course. A better example is an office environment where they put cameras into hallways for the obvious purpose of security. A dispute was raised about the fact that the employer had seen employees congregating for various purposes, be it union purposes or otherwise—

Mr DAVID SHOEBRIDGE: They saw that as dangerous, no doubt.

Ms LEVERINGTON: Yes, they saw that as dangerous. When those same employees requested that a camera be put in the dark underground car park so that employees could safely go to their cars at night, that was declined. For us, that really puts it in perspective.

Mr DAVID SHOEBRIDGE: So all future union meetings are in the car park. Is that right?

Ms LEVERINGTON: You know it. Yes.

Mr DAVID SHOEBRIDGE: Can I ask about the organisational structure? You spoke about moving to one entity, having both a reporting role of data breaches and also an implementation role in terms of ensuring cybersecurity. Can I put an alternate proposition to you? If the one agency is required to set and enforce the policy and also report when breaches happen and the policy fails, don't you have an inherent conflict of interest? You might be better off having the reporting of breaches in a separate agency like the Information Commissioner or the Privacy Commissioner.

The Hon. TREVOR KHAN: And an audit function by the Auditor-General or someone.

Ms LEVERINGTON: Yes, and each agency really needs to be required to report its own breaches, but we think that there needs to be a regulatory function within a department.

Mr DAVID SHOEBRIDGE: Yes. But if you are going to have one agency dealing with cybersecurity then there seems to me to be good arguments to have an agency that sets and implements the policies, perhaps with oversight through the Auditor-General. But if that system has failures and there are data breaches or the like, you would want the reporting and the oversight of the breaches to be done somewhere else so that you did not have a conflict of interest about enforcement.

Mr COSTA: That sounds sensible.

Ms LEVERINGTON: Yes, that sounds sensible.

The CHAIR: Thank you very much for your evidence NSW. That concludes our public hearing for today.

(The witnesses withdrew.)

The Committee adjourned at 15:02.