InnovationAus.com
Public Policy and Business Innovation

pwc

CYBER LEADERS ROUNDTABLE

BIG ISSUES FOR BOARDS AND DIRECTORS

Top row: Steve Ingram, Asia Pacific Cyber Lead, PwC; Craig Davies, Chief Executive Officer, Australian Cyber Security Growth Network; Helaine Leggat, Board Director, AISA; David Powell, General Manager, IT Security Strategy, NAB; Rachael Falk, Director, Technology Security and Strategy, .au Domain Administration; Peter Woollacott, Chief Executive Officer, Huntsman Security; Sally Ernst, Chief Executive Officer, Australian Cyber Security Network
Bottom row: Leonard Kleinman, Chief Cyber Security Advisor, RSA; Daniella Traino, Cyber Security Leader, Data61; Stuart Mort, Director, Cyber Security, Optus; Sunil Sharma, Director Digital Trust, PwC; Michelle Blum, Chief Executive Officer, Australia-Israel Chamber of Commerce; Robert Martin, Partner, Cyber & Forensics, PwC; James Riley, Editorial Director, InnovationAus.com

InnovationAus.com and **PwC** hosted an exclusive roundtable luncheon in Sydney with a leadership group of Australia's foremost thinkers on cyber security issues. These group Chief Executive Officers, Cyber Security Officers and Directors of IT Security came from a diverse range of industries.

The roundtable was organised as a forum for discussing the key issues shaping the future of Australia's cyber leaders.

Our participants came from backgrounds including banking, telecommunications, consulting and institutional research, while the discussion centred on topics like building best-practice frameworks for business/government collaboration to build cyber leadership skills; issues related to industry input into tertiary curriculum related to cyber; and engagement strategies for making cyber careers more attractive to a range of qualified professionals, from lawyers, to engineers, accountants and economists.

There was an on-going and important discussion about the critical need to build a pipeline of critical cyber-skills at all levels – from the TAFE graduates of generic ICT to the post-graduate qualified pure mathematics specialists.

A key talking point – and this is a topic we find again and again in any discussion about security issues – is the fundamental need to build genuine cyber leadership skills across the economy. While cyber security technical specialists are critical, of course, there is also a genuine need for cyber leadership skills in all job sectors, from healthcare to retail to financial services and tourism.

CYBER LEADERS ROUNDTABLE

BIG ISSUES FOR BOARDS AND DIRECTORS

This was a critical point of vigorous agreement among the attendees – that this issue goes beyond "cyber awareness". Generic awareness of cyber issues should be a given, a baseline need across any modern workforce. The cyber leadership skills across different professional disciplines and different sectors of the economy are a higher level, leadership need.

A subset of the need for improved cyber leadership across the economy was the recognition among the participants for improved frameworks for information sharing, between businesses, between sectors, between governments – and between government and business.

Everyone has a role to play in relation to cyber if Australia is to fully participate in the global digital economy, and as a continued technology and leader innovation leaders. That was a core agreement.

But there are significant challenges in designing and building the leadership frameworks that will deliver the cyber skills we need. These are challenges that cannot wait.

If there was a single message to come from this cyber leadership group, it is that in relation to Cyber Leadership skills development, the nation just needs to get on with it. All parts of the cyber ecosystem – indeed the wider economy – have a role to play.

And while the response to this national challenge might not be perfect initially, it just has to start. Now.

Following is an extract of the discussion.

CYBER LEADERS ROUNDTABLE

BIG ISSUES FOR BOARDS AND DIRECTORS

STEVE INGRAM: The best way is to develop a future cybersecurity work force for business and government is to share our thinking and share experience. We need to be asking how can government and private sector do that better together.

DAVE POWELL: [At the Cyber Leaders forum] we heard lots of talk about cyber talent and skills challenges. The bottom line is that we have just got to start somewhere. We can't solve what we haven't done.

We can whinge about not having enough security skills, but if you look at banks and other organisations, we actually do pretty well [in Australia]. It's the tier two and tier three banks where the biggest challenges lay. And no one is actually focused on any of this stuff so we need to be working together.

How do we, as big corporations, and government, help these industries, lift the skills and the talent? Let's just start focusing on the skills, so we can help people in the market.

[At NAB] we've done this with Boxhill TAFE, which Helaine [Leggat] and a few others have helped me implement. There is really a great syllabus with Boxhill TAFE, where we are involved. Right now we're funding six [people] and the intention that for the time that they're at the TAFE, they are also training with us, on a rotation system within our own team.

We will be able to give the skills sets they need, much like things like medical internships that are conducted at a TAFE level. When they when they finish their term, they hit the ground running and they're totally employable.

Now the theory is that when they finish, we don't employ them. Instead they get handed back to the industry to be employed elsewhere, fully trained. We may employ one or two – depending on how desperate we get and the holes we need to fill – but the intention is to hand them back into the industry.

In this way we are starting to invest in a framework and to say, how can we as big business support Australia [in the development of this critical talent]? We are also talking now to the Victoria Government [about this scheme] to get more Victorian big businesses behind it.

But we need to get bold with our thinking on how to get more graduate level skills through our universities. We need to get bolder with this stuff. And I am putting it forward that we should get rid of HECS debts for people studying cyber. We could just say no HECS debt for the next five years for cyber graduates. There you go, that would make a difference. This is not a new idea. It has been done previously in teaching and nursing.

And we've got to commit to some internship type programme to get these graduates ready. This is what we in business can do to actually get the skills set up. That will really start to change the game – and the numbers – if we can really start to pump these students through up there.

> *"We need to get bold about our thinking on how to get more graduate level skills through our universities …and I am putting it forward that we should get rid of HECS debts for people studying cyber"*
> ***Dave Powell, General Manager, IT Security Strategy, NAB***

CRAIG DAVIES: For us at the Australian Cyber Security Growth Network, education is going to be a really big thing, and Box Hill TAFE program is a really good example. I spent some time at the Boxhill TAFE a couple weeks ago. All the points you're raising are good. We want to build on those and do more.
We're bringing the tech community across Australia together to say 'Have a look at this stuff happening at Box Hill TAFE". We want to get a common approach happening and based on the people we've spoken to, the ongoing education will be more vocational in nature. Then we will have others coming in at various levels, and at Box Hill, most of the students actually didn't have an IT background at all. There was a chef, there was a waiter, there was a mechanic ... it was [incredible what's happening there.].

HELAINE LEGGAT: Boxhill TAFE has brought in people like AISA (Australian Information Security Association) and various other organisations to say, what is needed as the end result of a course? What kind of job must this person be able to perform [and what skills do they have to have]?

This has been really excellent because it is a process to manage the school's capability.

DANIELLA TRAINO: It also raises an interesting point. We're trying to get to the front lines with high school kids so that they see STEM and cyber as a vocation. There's an elephant in the room in relation to this: We're assuming that the education that is available today is combining the necessary skills that we actually need in the [cyber] industry today and in the future. I don't think we've really addressed that gap either.

There's a question of industry broadly working with a lot of those educational institutions to make sure the coursework is appropriate for the jobs and the skills of the future. Not necessarily a particular role because that could change, but the broad skill set you need.

I look at other examples, and I'm not picking on the financial institutions,

Cont...

but the Commonwealth Bank is orking with UNSW for security engineering costs. That's not the only example, but it's one where you see there is a gap in engineering skills in cyber security and instead of bemoaning it, [the industry] works with them, get the curriculum up to date and make sure that you can [create a] funnel of talent.

CRAIG DAVIES: One of the challenges we have in the Australian industry is that lots of people are trying to do lots of things, and it kind of goes into an environment [that can create] misfires. That's where we're [at ACSGN] are being creative. I talk a lot about harmonising the approach, not standardising, but harmonising the approach. We want to try and stop the top-down approach.

"One of the challenges we have in the Australian industry is that lots of people are trying to do lots of things, and it kind of goes into an environment [that can create] misfires."
Craig Davies, Australian Cyber Security Growth Network

SALLY ERNST: Basically growing our digital economy while making it safer. Any large business or small medium sized business is going to have a lot of difficulty developing something safely. They will, however, engage on the dot point of innovation, so if we can engage with them on innovation and then we can build cyber security into the back-end. But how do we do that?

There's an opportunity there to solve large businesses problems, including financial institutions. Once we start embedding [cyber thinking] into the backend of corporate innovation – where assets can be leveraged at a lower marginal cost – [then] we can start achieving some of Craig's objectives.

But next to that, when you look at things like Optus is doing with Macquarie University – and I've pushing Macquarie some time down this path – this is an opportunity for universities to engage with corporates, which helps the university. It allows innovators to get access to researchers and ultimately, we get this upwards spiral of growing our digital economy, while making it safe.

SUNIL SHARMA: Once kids are in the university system, they've already thought about what they want to do. We need to start the discussion about security much earlier. We need to start educating them and making them aware of security issues at school.

That way if they're looking at medicine, or if they're looking at being a financial accountant or whatever, they can see how security issues relate to those functions. That awareness itself will get them thinking.

CRAIG DAVIES: We've also got a few things happening. I'm a great fan of experimenting, so there'll be some announcements coming out of South Australia in the next couple of weeks.

RACHAEL FALK: I think you have got to look at what problems you're trying to solve. The first thing is, are you trying to solve – to take your point and start somewhere – diversity? Diversity is a broader issue [but addressing it also helps improve raw numbers of cyber skills].

Number two, we again kind of fall into the tech trap and I would encourage everyone here again, to not go down on that road. We don't have enough tech people; I would challenge that. Remember there's a collision coming. You're going have all these tech graduates. In that, you have to multi-skill them so that they aren't just cyber security, they can potentially be critical thinkers who understand the broader ramifications of [cyber issues across the economy], along with forward thinkers because not everyone will be a doctor or a lawyer and they don't want to be.

What did we need to do differently? Are you giving people just jobs or are you offering them a career? What is different for women? What do women look for [in these roles] as opposed to men?

I don't know the answers. I'm just saying, are you attracting law grads and saying, "We can't offer you a career in law but what we can do is help you solve hard problems."

PETER WOOLLACOTT: This is not surprising in an emerging industry. We're looking for ways to feed and support and populate the industry. I just wonder whether young people who are looking to access this industry don't know which door to push on to find a career, whether that's a TAFE level career or university.

In years 11 and 12, how does someone who thinks they have got a disposition for cyber security get started? They will have the question … 'where do I go? What courses can I do? I don't think that we are providing a road map for kids to get started on the treadmill. It's all very random.

STUART MORT: That's a really good point and that's where the cross skilling is important. Some come from the legal profession into cyber security. And they are the kind of people that we need to go and speak about this, not the hardcore cyber historians like us, but in terms [people who have] transitioned from a legal career into a cyber career.

We also need to think about how we create the finances for someone to step out of a waitering position into cyber. Singapore, for example, would offer a 70 per cent discount on cyber courses for their citizens if they want to make the transition into cyber. So it's not just about bringing up the graduates or encouraging people to do undergraduate courses in cyber. It's also about looking at people that already have degrees or have a skill set in a particular area, and [helping to] transition them across.

"It's not just about bringing up the graduates or encouraging people to do undergraduate courses in cyber. It's also about looking at people that already have degrees or have a skill set in a particular area, and [helping to] transition them across."
Stuart Mort, Director Cyber Security, Optus

Cont…

DANIELLA TRAINO: It's also the why, right? Because we don't actually make it really clear to

people why would you look at cyber security as a career choice. That's why Life Journey is an interesting mix, because if you look at outback brands, they're not linear. They're not exactly the same. They fell into the industry.

There are people out there with immense skills that would find this a really interesting career choice if we made it clear to them. As hiring managers, and I see this all the time, we need to broaden our perspective as well. The way we hire for cyber security professionals or cyber skills is very black and white. It's very old style.

And yet, the skills that I've seen are much broader in people. As hiring managers we need to be broader as well, and there are still some organisations that are very dogmatic.

SUNIL SHARMA: You're competing for Generation x, y and z, so you need to be able to relate to them as to how it's going to affect whatever they're interested in. How does cyber really fit?

Unless you try and relate them to what business needs it actually fulfils, and it doesn't matter which discipline you're going into, law or business or medicine or whatever it is – how does cyber actually relate to that?

So that they have an open mind that while they're doing medicine, they might do cyber as a second subject, and it might become a career later.

MICHELLE BLUM: It's interesting also to look at the Israel experience where the whole thing is not about an education pathway at all. Obviously the great success of that industry [in Israel] has been drawn from the military and the expertise that's gained by these 18, 19, 20 year olds in intelligence where they really learn these strong skills around critical thinking.

There's no formal education that's gotten them to that point. They are learning in a very agile environment and dealing with very sophisticated threats where they are given leadership opportunities. I think looking at that out of the box sort of approach where we have obviously capabilities in other spaces – whether it's in our defence forces or our police forces who are also gaining these skills – or equally in these other areas where people are learning those critical thinking skills. This is really a key theme, that it's informal training coming out so start helping to accelerate the influx of people into this area.

> *"It's interesting also to look at the Israel experience where the whole thing is not about an education pathway at all…they are learning in a very agile environment and dealing with very sophisticated threats where they are given leadership opportunities."*
> ***Michelle Blum, CEO, Australia-Israel Chamber of Commerce***

CRAIG DAVIES: We were talking before about Life Journey and I think this is a really important thing because it actually doesn't talk about technology at all, it talks about the journey and all the different opportunities that are there and they've had incredible success in the U.S. So we're getting a proven program that's been adapted.

The biggest challenge I'm having at the moment is finding out about things that are going on and then for whatever reason, people think it's a turf war. It's not [and I am telling people] 'you need to work with me on this'.

We're going to make it super successful. That's my biggest mission is around how we get these people together and put them in a room and go, "Right. Let's figure this out."

STEVE INGRAM: Perhaps a turf war is a result of a void.People have stepped up to fill that void.

CRAIG DAVIES: Australians struggle to truly understand the 'shared' idea.

HELAINE LEGGAT: It's always so competitive, particularly in the universities and through AISA, we have a number of people that everybody wants to be there first. I think that the area in which we work moves so quickly, the problem is that more and more people can't keep up. The competencies you need for tomorrow's threats are very different from today.

The legal profession is like that too. You learn the basic legal stuff, but then when you get a job, it's all about knowing where to find stuff, and going out and researching. That's really the nature of cyber.

CRAIG DAVIES: The skills need to be at the critical thinking level so that's going to evolve very quickly. The other challenge we have as a country is that we have just got to get a move on.

That's what makes it really exciting and I want us to experiment in a few things. I want people to work with the universities. We should try this and go, "Okay, so what did we learn from it?" We want to get a much more rapid cycle of that experimentation happening. That way we can feed it back into the system and go, "Okay, that was really good. That worked quite well. What's the next version look like?"

DAVE POWELL: Let's start. That's my point. Let's agree on a TAFE course, let's agree on a syllabus for a degree course, and let's go with Life Journey as a start to actually get the hearts and minds and get more young people to understand what a cyber industry is all about.

RACHAEL FALK: It is about sharing more stories. It is about the possibilities that people need to see.

They don't see the linkages to the cyber industry. I practised law for 15 years. When I did my Master's in National Security Policy – which was a deliberate thing to do after law [and that's how I started into cyber] – they put me up as one of their first sets of students who are on the website. and I heard that somebody who was also a lawyer at the time read it and said, "I want to do that Master's if Rachael is doing it and she's a former lawyer. I'll do it."

Cont…

Whether it's just more about getting out there and telling stories and everyone in your organisation, you have bright people that have amazing past lives, get them all out there and just get them to go to talk to unis and share stories.

STEVE INGRAM: Two or three years ago, doing an inclusive program at work, I had this very uncomfortable recognition. I realised that when my children came home, I'd react positively to my son's news about math or science and I'd react positively for my daughter's news about art or English. And I didn't reverse it.

I never set out to do that. It was just my hard wiring, I guess. So I think we're doing modelling but then I'm wondering, do we have a convergence of revolutions here? This is clearly a revolution beyond the industrial revolution.

Technology coming right into even the most intimate part of our lives, into medical devices inserted inside of us. We have got to deal with that [from a cyber perspective]. And we have got to deal with a more dynamic, changing workforce … because put your hands up, those of you that have been in cyber since they left school. No one.

PETER WOOLLACOTT: That's the important thing that I'd say. There is an enormous diversity of careers around this table, and yet, we're all bonded together by something as simple as cyber security.

I'm a structural engineer who left university with a hard hat and gum boots. It epitomises what we're all doing here today. The fact is that cyber security is just a core part of where we're going as a society and as an economy. And so we need to hurry up and get kids knowledgeable about it. We need to inform them [about] the opportunities, and we need to get people on board. There needs to be some coordinated talking, because this needs to get some scale as quickly as possible.

"The fact is that cyber security is just a core part of where we're going as a society and as an economy. And so we need to hurry up and get kids knowledgeable about it."
Peter Woollacott, CEO, Huntsman Security

LEN KLEINMAN: I know from my previous experience that when you're recruiting these people, it's not about into cyber. It might be one of the first questions you say, "What's attracted you to apply? What would you say is going to be your forte?" Within cyber there are so many different streams. You have to tease them out. I know people say, "I want to be a penetration tester." Another says, "No, I want to actually understand enough," probably to your point, "to become a trusted advisor at some point." Someone else just wants to be an incident responder. There's diversity under that bough of cyber.

RACHAEL FALK: I had the luxury in a previous role of establishing a new team, a cyber influence team. I had one of my guys – who everyone loved – just going in there talking to people. He was almost like this secret agent that I'd send out. That's really important, to get out into an organisation and talk to people, to understand what projects they are working on.

Because we were the influence team and part of that was – I would use any form of influence to gain intelligence, to find out what was going on, to work out how I could get to people better. You need to understand exactly what people are working on in the organisation in order to have the influence you need in relation to cyber. You have to engage with people.

I had to eyeball people more, because a lot of guys just didn't want to talk. And I had to engage more because I realised that was the way I was going to start to interact with every gamut [of the organisation]. I had been a closeted lawyer who was use to [just dealing with other lawyers and clients.] But now I had to move differently, and learn a different dynamic in order to engage the techies, but they still wouldn't give up the kernels of what they were wanting to tell me. But I learnt that the best way is – and it was a good lesson for me – go and just engage, and to be friends. You don't have to be best friends with chiefs of staff and everyone. Just be their friend.

STEVE INGRAM: I can endorse that. Most of the successful CEO's I see are actually ambassadors. They're really spokesmen for that business.

CRAIG DAVIES: Australian universities are getting a good balance happening and there will be a blend. You can pick the universities now, so UNSW with their education will naturally fall a little bit more to the technical side, because that's where they are. Whereas Macquarie will head a little bit more into the human sciences, because that's where they are.

I like the fact that I've just seen the first 10 people that I'm going to do an interview with and they're going to put it on our YouTube channel, which I'm hoping to launch in the coming months... But that's the way you do it. You win by starting to tell stories. People need to connect.

STEVE INGRAM: Israeli companies setup in Israel and move out, whereas Australians startups go to the U.S.

CRAIG DAVIES: Because that's where the money is.

STEVE INGRAM: Not only that. We've got a different outlook from the start. We're not surrounded by enemies. We don't have the same depth of national focus or concerns that a lot of those do in Israel, quite rightly. We're not that worried about New Zealand.

SALLY ERNST: That's why I say, can we get the deal flow so that we get the insight on the innovation, which is the next wave of either cyber security solution or where we want to tuck cyber security in. Can we leverage the infrastructure of the larger organisations and can we pull in some identification programs for startups. Even TAFE actually, Queensland, has a cert for mentorship.

STUART MORT: What we're trying to do is mentor these startups, [to help them find a way to sell into large organisations without going broke in the process.] If I can see they've got some great tech which I know I can map into some of my

Cont…

strategic customers – but who won't buy from them because of the risk – then we try to do that. So we'll sign up the startups into Optus, and so we cover the risk, and we wholesale them to our customers.

CRAIG DAVIES: We recently released a sector competitiveness plan around where we see the opportunity for the Australian market, and where we can go with it. If you have not read it, please do. We've mapped out a lot of these areas. We literally only launched it a bit over a week ago. And there's lots of opportunities. It was great that Senator Sinodinos was [at the Cyber Leaders forum].

DANIELLA TRAINO: If I could make an observation just in the R&D space, I think there is a lot of talent in this country, which we need to build on. But unless Australian-based organisations can reduce the stigma of dealing with R&D organisations here [then we are missing an opportunity].

But it's interesting because even in my job, most of the interest is out of Australia and the IP comes back, the innovation comes back through an American company or a UK company, because Australians don't value the IP that's here – or actually don't even know how to interact with it at times.

STEVE INGRAM: We've talked about how we build a cyber workforce. We've talked about how to create a curriculum. We've talked a bit about startups and education … but how do we look for what the next wave of technology is that Australia could benefit from? How would we go about finding that?

DANIELLA TRAINO: The observation I'd make is that it's not about the technology. It's actually about the problem you're trying to solve.

We have incredible innovations, some at the very early cusp and machine learning is very early stages. We've just seen the basics. There's some really impressive stuff coming, but there are also a number of concerns with AI and machine learning and things in cyber that we haven't really explored yet.

Even basic things around how we transmit our biases into a lot of what we develop and what does that therefore mean for our use of it. There are some really funky things that are happening here and Australia is part of that discussion. It's part of that innovation but I go back to basic principles. It's not about the tech but what is the problem you're trying to solve.

What society are you trying to create? And therefore, what do we actually need to create that? The technology will be a driver for it, but there'll be a whole manner of other things that we'll need to think differently about – with regards to policy, with regards to legal, with regards to society norms and including in cyber specifically.

But again, I go back to what is the problem we're trying to solve. In cyber, from where I sit in the R&D space, what I see is there's a huge opportunity for Australia to take the lead in thinking about these problems very differently – because we're a very different community here. We don't have the scale of the US, we don't have the funding necessarily that you have in Europe. Therefore, we have to think about how we can solve these challenges quite differently. And even what I'm seeing around information sharing, we think about that problem differently and that scales globally.

I think there's a huge role for organisations like those around the table, to look at those problems in cyber we're having today and say what is it we need to do to actually push the envelope. And not a step change either, but a revolutionary one. What is that?

STEVE INGRAM: What would that outlook look like?

DANIELLA TRAINO: I would say as a starting point, there's a set of problems that are things that we're band-aiding today, things that you can see coming down because your business wants to be pushing the boundaries in certain ways, wants to be accessing your customers in a certain way, wants to be providing those different services.

Those conversations don't need to be technical per se, but we need to agree on what are those problems? And there are some industries in Australia – like mining and agriculture – that can actually give you great stepping stones to apply that thinking, and then take those things globally. That's just something to think about.

We can talk about the tech that'll come – and there are some amazing things that will come – but that's just looking for a problem to solve.

SUNIL SHARMA: Just to add to that as well, Rachel you brought in your talk today that although attacks are becoming sophisticated, I think your message was let's get the basics sorted. I feel 70-80 per cent of the organisations still today are not doing the basics right. Depends on where you're trying to target and if you're going into financial services organisation, yes they're doing something better but again, some of them as well are not getting the basics right.

DANIELLA TRAINO: The basics, we give them really bad tools to do the basics. If you look at identity, we tell people to remember complex passwords and change them daily. Or we use tokens or we use this and then we confuse consumers and we confuse our corporate users. That's a problem we should be looking to solve, trying to make that easier, but also have strength in the method.

LEN KLEINMAN: I think that what we're getting at is basic security hygiene. I have to agree. There's an abstract layer here, in the sense that there are organisations out there right now that don't fix the rudimentary, fundamental, basic vulnerabilities – and yet they know about them. It's basics here.

STEVE INGRAM: My takeout from that last question we persevered with was rather focusing just on all the new technology that's coming in, we should look at the emerging problems that we have to solve.
Finally, let's go around the table for a final closing comment of 30 seconds or less.

Cont…

RACHAEL FALK: First. Cyber security is a complex thing. I think we keep on having the conversations and sharing stories. We just keep on. Let's all commit to sharing stories.

"Sharing stories. We just keep on. Let's all commit to sharing stories."
Rachael Falk, Director Technology, Security & Strategy, .au Domain Administration

ROBERT MARTIN: It's the people. Better psychology of people.

MICHELLE BLUM: I guess as the CEO of the Australia-Israel Chamber of Commerce, we're very happy to support this evolution of the ecosystem here in Australia. That is something that has to happen.

STUART MORT: I'll expand on the human aspect – it is a business problem. It needs much more board level awareness, and there are too many boards that are discussing cyber when in my opinion they are 10-15 years too late. We need to change that.

SALLY ERNST: How can we grow our digital economy while making it safer? And leverage, under a joined-up approach, what already exists and in that context, as you're going out and finding and having the real conversations and finding out what it is.

SUNIL SHARMA: I think cyber security needs to be about making it more relevant to what you're trying to achieve. It's about the people you're hiring and diversity of self needs to be done through education and awareness rather than pushing it down and saying, "Ladies, let's join." Let's spread that across because even the younger men, they're not very keen on looking at cyber security, even though they might be down the track so it's really about educating them.

PETER WOOLLACOTT: There is no question that we need to keep spreading the word about cyber issues now. Whether it's spreading the word at young people who are looking to enter the industry or whether it's spreading the word with senior executives and board members, who are starting to grasp the concept but we've got a long way to go and I have this personal theory that the reason that cyber insurance is such a successful product right now, is because board members still don't understand cyber risk and so we've got a long way to go and we need to keep working to achieve that.

JAMES RILEY: A lot of the conversations that we've had, very fascinating conversations around training, attracting young people, attracting the best and brightest, translational issues, research into the commercial world, are all conversations that we've had before. I guess the difference now in cyber security is that it has been made a focus of the government. That intense focus has really only been in the past 12 months and there has been great progress in that period, and we're happy that we can continue that.

DANIELLA TRAINO: I look forward to having a slightly different conversation around cyber security in that, the problems that we've known for 15-plus years, we haven't changed the dial and there's no reason why Australia can't be leading that pack or part of that pack in the innovation ecosystem, if we get some of the infrastructure right particularly but I look at what Data61 does, its network, and organisations like this around the table and there's no reason why we cannot make a difference in cyber security with tools, people, techniques, etc to change that conversation so we're not talking about the same things in another five or 10 years.

LEN KLEINMAN: I'll just say that the cyber security ecosystem has got so many hidden parts of it but the most common thing that we all have is the people aspect, we need the right people with the right skill sets in the right places, including the Board.

"We need the right people with the right skill sets in the right places, including the Board."
Len Kleinman, Senior Cyber Security Advisor, RSA

CRAIG DAVIES: Geez, I've never done 30 seconds or less. The one thing is with all this conversation and everything, which is wonderful, I always enjoy it. The government has given me what many people think is an impossible mission. We can't do all the things all at once so you need to help me to prioritise those things and from the prime minister down, they are keen to really drive this home and we do talk about really important things. These are all important. I want to fix the skills problem. I want to fix the hiring problem. I want to fix the technical problem. I've worked in this field for a really long time but as a community, we need to go, "Can we focus on this thing first? And then let's get that moving and then we'll try something else." And we'll try lots of things but we don't have all the answers yet and we will never have all the answers so all I ask from everybody is ... We're still having a little bit of conversation across the community. We should do a thing. We actually are doing a thing so your homework is to have a look at the sector plan.

DAVE POWEL: I urge people to get behind the skill shortage. You know that's my thing. There are many other issues that I've got but that's my primary one. Let's just get behind some things that we can go and work with Craig on to actually solve.

That's my primary thing and secondly thanks so much to Steve and PWC because this has been one of the better discussions. I attend a few of these and this has been one of the better forums where we've got the right people in the room to actually start making a difference for some of these issues and keeping it on track so that we don't go too far off on active defence and other issues.

STEVE INGRAM: My closing words are that we're a tough nation on ourselves, we really are. We don't celebrate success. We always think we're wanting and someone mentioned before, Australia is like a canary in a cage. I look at my experience with PwC. Australia does some amazing stuff and I think we actually punch above our weight.

I feel, and the discussion today has really brought up to me as well, there's a few revolutions converging here and we can't ignore that. There is an industrial revolution. There's an employment or an expectations revolution. There is a gender revolution to get the balance right. I think they're all converging and whilst many things have happened out of coordination, I think they've happened because we've seen a gap and we've all stepped up to fill the void. I'd say that if we want to take something forward, it's to be open and if we put effort into an initiative, it's to bring those initiatives together with others and not think anyone's failed or done the wrong thing, to actually one plus one can equal three and to make Australia seriously a better place to do business.

There are a few revolutions converging here…I think they're all converging and whilst many things have happened out of coordination, I think they've happened because we've seen a gap and we've all stepped up to fill the void.
Steve Ingram, Asia Pacific Lead, PwC