**Public Sector Future WWPS Podcast**

**Detail: Cybersecurity mini-series podcast**

**Episode: TBD**

**Host: Alvaro Vitta**

**Guest: Dr. Marcus Thompson (Cyber Compass)**

**TRT: 30:53**

**Audio: Public Sector Future\_Cybersecurity\_EPTBD\_Marcus Thompson\_V1**

[TCR 00:00:00]

[Music.]

[TCR 00:00:09]

**OLIVIA NEAL:** Hello, and welcome to Public Sector Future. This is a show for anyone who cares about using digital approaches in the public sector to deliver better outcomes. I’m your regular host, Olivia Neal.

Today we’re continuing our set of episodes on cybersecurity, and we’re going to be hearing from Dr Marcus Thompson. Marcus is a retired Major General and former Head of Information Warfare for the Australian Defense Force. He’s going to be talking to our guest host Alvaro Vitta, who you met last time, about his lessons from his time in the military, and how he recommends public sector organizations can be better prepared to protect sensitive data.

[TCR 00:00:28]

[Music.]

[TCR 00:01:19]

**ALVARO VITTA:** Well, thank you for joining us, Marcus, and we’re glad to have you here.

**DR. MARCUS THOMPSON:** It’s my absolute pleasure, Alvaro. Great to meet you and fabulous to be a part of this wonderful Microsoft initiative.

**ALVARO VITTA:** So Marcus, maybe start also by telling us a little bit about how you got into cybersecurity and working with government organizations?

**DR. MARCUS THOMPSON:** Yeah, sure. I did 34 years in the Australian Army and finished in January 2021, after, I said 34 years. So I grew up in the Royal Australian Corps of Signals. That’s the part of our army that does all of the information and communication technologies for the combat force.

I was electrical engineer by trade, and I grew up in that organization, so quite literally, you know, well over half my life and certainly

But through all of that, you know, a – an amalgam of my operational experience, my – my technical qualifications, knowledge and experience, I got really interested in cybersecurity, just before it was – before it became trendy to – to do so, if I can use that phrase.

And so, I ended up completing a PhD in – in cybersecurity, which – which then prompted our Chief of Army to give me a job of raising our army’s cyber capabilities. And then having done that, I was promoted to major general and given the task of doing that for the entire Australian Defence Force.

And so my final appointment in uniform was as the Head of Information and Warfare for the Australian Defence Force, where I had capability management responsibilities for military cyber, electronic warfare, and some other capabilities that are all related. I did that job for four years.

So as I said, after I finished in the Australian military in January last year, January 21, and since then have – have compiled a portfolio of responsibilities, you know, different board roles and advisory roles all on the theme of cybersecurity and in making sure that the best capabilities are available in Australia, but also looking for opportunities to bring in, you know, the best foreign tech for use in in an Australian context.

[TCR 00:04:07]

**ALVARO VITTA:** And that’s quite a diverse set of experience. And – and we thank you for your service, by the way. And you bring a plethora of mission-driven capabilities that, of course, a lot of organizations, government and nongovernment, would leverage going forward from you.

**DR. MARCUS THOMPSON:** I find myself, reflecting on, you know, what just lessons that I’ve learned in the – in the past 18 months since leaving the military and leaving government service, and I think that there are some really, you know, helpful observations, that I think I’ve got my former colleagues, you know, certainly in the Australian Department of Defense and elsewhere, and you know, could use and –

the biggest observation I’ve had, mate, is that – is that I think industry can do more, you know, and government can facilitate industry doing more. And I think the key thing here is, let government do what only government can do, and then look for opportunities to bring industry in to help with the rest.

because I think –– that deep technical expertise that resides within – within industry, I think the – the ability of industry to innovate, and innovate at scale, is – just remains something that I think certainly in Australia government could perhaps do a bit better. You know, the bureaucrats could actually be a – be a bit better with that.

Now, I’d use myself as an example here. I mean, there was a time when I thought that certainly when it came to cyber capabilities, there was a time when I thought that the national expertise resided within government, within the Australian public sector. You know, so as I’ve stepped out of government, I’ve realized just how wrong I was. And so, I do find myself evangelizing just a little bit on this in helping my former colleagues within the Australian system of government to – to understand the capabilities that exist within industry.

[06:15]

**ALVARO VITTA:** I agree, Marcus. I think that tends to happen, right? Human nature is that we tend to focus, especially in cybersecurity, right, and if we’ve been in that space for a while. And if I’ve been in government, let’s say for, you know, 15 years, you know, running security operation centers, and standing everything from the ground up, and getting everything up and running, I feel like I have everything under control, and I know everything that there is to know.

And so, I fully agree in that ability to understand that there may be other organizations or other peripheries that you don’t know, are super important in being humble and understanding that, hey, let me go out there and see what’s out there and maybe incorporate some of that in here, as I incorporate some or what I know to them as well.

[07:11]

**DR. MARCUS THOMPSON:** Yeah, albeit, I mean, I absolutely agree with you, but there are times when it’s not easy, right? When you’ve got folk working in government, you know, these are – these are smart, professional people with – you know, who are working hard with the very, very best of intentions. and I was the same, mate. I remember this. You know, you’re just so busy.

I wouldn’t profess for one minute to think that I mastered that while I was in government service, but it is – it is, it’s really important to do, right, you know, is just taking that moment just to lift your eyes, lift your gaze, lift your focus, and just have a quick scan out just to check you’re not missing something.

[07:51]

**ALVARO VITTA:** In your experience, Marcus, cybersecurity, as you know, is a huge field, right? It’s massive, and there’s a lot of different areas. But at the end of the day, adversaries, cyber-attackers, want data, right, that is the currency that they’re after.

I wanted to get your sense of experience in coming from the military and working with governments. What are some of the most common needs and challenges that government organizations have, as they try to protect their sensitive data, while having to use that data?

**DR. MARCUS THOMPSON:** Yeah, well, I mean, goodness me, right, I mean, that’s a big question. I mean, we could talk for hours on that – on that alone. But look – but let me – let me offer a couple of observations.

I mean, I think one of the things that I still see and that, you know, and seriously, mate, this kills me, is I still see plenty of apathy in some areas of government. so I say to anyone who’s prepared to listen, you know, just remember here, you know, that there is a threat, there is a cybersecurity threat out there. The threat is real, the threat is active, and it wishes you harm, it wishes your organization harm, it wishes your family harm, it wishes your nation harm. And I think all good comprehensive approaches to cybersecurity start with a recognition that the threat is real, that it’s active, and that it wishes you harm.

And then you go okay, well, all right, okay, yep, thanks, Marcus. I – I accept that that Yep, I’ll recognize that there’s a threat. Well, so what do I doing now?

and that can be a real challenge for smart generalists, you know, people who are not cybersecurity experts. And for mine, I just encourage smart generalists, you know, leaders, policy people, resource allocators, you know, people who are intelligent senior leaders, but perhaps, you know, who recognize that cybersecurity is important, are prepared to invest in it, accept that they need to invest in it, but don’t really have a clue where to start.

I’ll just say, right, thinking of these in these three headings. Think about your self-defense, think about your passive defense, and think about your active defense, and just as – as a conceptual framework, for thinking about the adopting of a comprehensive cybersecurity strategy.

-

You know, what are we posting on social media, what are we freely giving away to the internet at, organizationally, or is – what is our workforce doing, that – that a professional threat actor, with a targeting mindset can turn around and use against us to – to attack us, you know socially-engineered phishing campaigns,. It’s about culture and awareness, and so, so a side effect, well, okay, so when you’re thinking about your self-defense, have a look at your culture. What are you doing, and either you can just continue to bang the drum about – about the importance of cybersecurity and encouraging all of their workforce to not be the weakest link, right? That’s self-defense.

Passive defense, I mean this is the domain of our system administrators, our CIOs, and maybe our CISOs. This is where we think, you know, how’s our network hygiene? Are we patching our systems? Are we patching our hardware? Are we patching our software? Do we have multifactorial authentication in—incremented within our organization? How many people have administrator rights, you know, have that privileged access, who might then become a potential sort of insider threat?

, these are just questions that smart generalists can be asking of your senior leaders and your senior decision makers, or indeed your technical staff. So, that’s the passive defense, and then the active defense – well, this is the bit where we say, all right, we know that if we implement good hygiene, good network hygiene, we’re patching, we’ve got multifactorial authentication and all that, all those important functions, you know, there’s still a chance that a, that a sophisticated threat actor can get in, can get past those defenses, so what have we got?

Do we have a highly capable security operations center, you know, the ultimate risk mitigator, you know, looking at our infrastructure to immediately detect, contain and resolve any penetrations, any breaches of – of our security? There was a – I think it was a – an IBM report, only a couple of months ago that said that the – this was in Australia, that the average time to detect and resolve a network intrusion in the Australian economy was some 311 days. You know, that was the average time, and that was not distinguishing between commercial, not-for-profit, government. I mean, that was, that was broader, and I get, mate, that there is this lie – damned lies and statistics, but that was the figure.

311 days is the average, you know, I shudder to think, you know, what’s happening at the – at the other extreme, and I – so again, to say that to smart generalists who are in positions of authority, you know, are you happy not to have a threat actor inside your infrastructure for that amount of time?

if not, then be thinking about your self-defense, your passive defense, and then do not forget about active defense; it’s really important.

[13:36]

**ALVARO VITTA:** I love that, those three, and I would say, within those three, I would put like a horizontal line across all of them, of zero trust. Why? Because, if you’re looking at, you know, self-defense, and in humans to make decisions, you know, talking about stats, one of the things that the stat shows, is that 34% of security incidents happen because of insider threats, right?

So if you don’t care to begin with, or you have either malicious intent, or disgruntled employees, or you accidentally do something, then that kind of becomes a – a weak link. Then the other aspect of that is that, you know, 80% or so of security incidents still happen, Marcus, because of malpractice and what you were talking about, in cyber hygiene.

**DR. MARCUS THOMPSON:**

We do what’s called a mission, you know, to use the military lexicon, and – and I think that’s where – you know, sort of back to one of my earlier points is things that only government can do, well, then, hey, government, get on and do it, you know, and do it really, really well.

But where there are opportunities to bring in industry partners, especially trusted industry partners, you know, and, and giving the opportunity to develop that trust with industry partners, then do that. You know, so having, having folk come in to run tabletop exercises, having folk come in to run, you know, simulated phishing campaigns.

having folk come in to red team systems and networks, you know, the IT, the information technology and the OT, the operating technology, and you know, setting the baseline for cybersecurity, you know, what the Australian Department of Defense calls cyber worthiness, that is the minimum standard that any system or – or network needs to meet before it’s fit to deploy, you know, across – you know, when we talk about military operating technology, we’re talking about, you know, ships, fighter jets and tanks, that these days are all, you know, complex digital platforms, you know, that are - running multiple networks that they all radiate, that therefore can be seen, and that therefore potentially might be vulnerable to attacks, even through cyberspace.

So, so all of that is assuming that baseline is really important, and then of course, you know, that’s the trust bit, well, then it’s verified, right, so you know, when there’s a new piece of malware on the streets every seven to twelve seconds, it’s all well and good to say, right, you know, we’re good, we’re in a good place here, you know, it, you might be just a couple of nanoseconds away from – from that not being the case, so back to that active defense piece of having folk actually look at your infrastructure to quickly detect any anomalies, detect any challenges, and resolve them.

[16:38]

**ALVARO VITTA:** That’s great, and yeah, I agree with you, you know, when we’re talking about prioritizing.

You can start fixing those, right, that are easy to fix and may have high impact, while you continue with your roadmap of getting at the other things that you’re going to have.

[TCR 00:17:00]

**DR. MARCUS THOMPSON:** Dead right, and – the approach must be a risk-based approach. You know, a compliance-based approach does not work in this – in this environment, in my assessment. when there’s a new piece of malware on the streets, every seven to twelve seconds, you know, you might be compliant, you know, but at – at that nanosecond, in that instant, you might be compliant, but a moment later, you’re now being noncompliant, and that’s where bringing a risk-based approach, that where the leaders of an organization, and it doesn’t matter if we’re talking about a – a large-scale commercial business, or a large government department, or a small government agency, it’s rather, what is our risk tolerance?

And therefore, what investment do we need to make to bring our risk down to within our tolerance, and the cybersecurity risk needs to be balanced against every other risk that every organization that needs to manage, and the investment to to bring that cybersecurity risk to within tolerance needs to be balancing every other investment that your organization is making.

It is not possible to bring the cybersecurity risk to zero. That’s, that’s just not a thing, so you know, a sensible conversation amongst leadership groups about cybersecurity risk, what we tolerate, what we can’t tolerate, therefore, what we need to invest, you know, today and into the future., these are sensible discussions that smart generalists can have, within government and outside government, and you don’t need to be a cybersecurity Jedi to have those, have those sensible conversations.

[18:46]

**ALVARO VITTA:** Measure risk, quantify it and make decisions based on risk, just like any – any executive should do, right?

**DR. MARCUS THOMPSON:** And then monitor it, and then continue to monitor it, you know, are our settings right? You know, are we being true to our stated tolerance? Is our investment right? Is there something new that has changed our risk landscape, and these are right now in Australia, you know, these are standard agenda items at board meetings, you know, for – you know, for commercial entities or – and government entities, , especially those who are now classified as critical infrastructure within Australia.

[TCR 00:19:22]

**ALVARO VITTA:** That’s great to hear, that’s awesome, that’s progress. So Marcus, as you look at your experience with public sector organizations, your own and those – those that you advise, what would you say are some of the pitfalls that you see in general, right, that government organizations should avoid when implementing a data protection program? And what are some of the principles that you use yourself to advise them, or that you have used in the past, to implement a data protection program?

**DR. MARCUS THOMPSON:** Again, Alvaro, I mean,, that’s a significant question that we could spend hours and hours talking about, the big one for me is I still see folk – you know, and especially in government, thinking they can do everything, and it’s just – you know, it – that’s just really hard, , we’ve got, I’m sure it’s well, in fact, I know it’s the same, you know, around the world, but I’ll keep my commentary to Australia where, we’ve got a significant workforce shortage when it comes to cybersecurity professionals in – in Australia.

My personal observation, anecdotally, you know, is that we’re probably 30 to 35% underdone in terms of the number of quality cybersecurity professionals that we need here to defend our economy.

So, so I think the – yeah, so I might just dwell here, for a minute, Alvaro, on workforce management because I know that there’s plenty of cybersecurity professionals work within government, just as there are plenty of cybersecurity professionals who work outside of government.

And I’d just offer that this is a unique workforce. You know, this is a – this is a workforce that, that is naturally curious, that is in a hurry, and that, you know, if we can put it frankly, knows its value. And, you know, the curiosity piece means that they’re always looking to develop new skills. And if you’re not, if you’re not a big enough organization hold internallyto hold a subsidiary workforce of sufficient size to satisfy that curiosity and provide those career opportunities for these individuals, then they will go somewhere else. so I sort of say, in effect, look, especially if you’re a small government entity, don’t try and do this yourself. Bring in the experts to do it – to do it for you, and let that workforce management challenge be their problem, not – not yours, because I think beyond the really big government entities, it is really hard to hold that sort of capability internally.

And so, that’s why question number one for self here is a – if I was working in a government entity, and it was am I large enough, do I have the resources to hold that capability internally or should I bring in a third party to do that for me.

Again, back to my earlier point, let government do what only government can do. Then look for opportunities to bring in industry elsewhere. I know it’s not cheap, but you know, back to level investment, level of risk, you know, where’s my tolerances? where’s the sweet spot? And I think that’s, you know, that’s probably one of the most significant challenges that I see here in Australia and chatting with my – my mates overseas. I see similar things.

Now, you asked specifically about data protection plans. One of the other challenges that I see and find myself advising folk about is, is this that first step of assessing and analyzing what data do I have that is of value to a threat actor, because it’s not everything, right? You know, I mean, for people who have their e-mail address and their mobile phone number on a business card or on their LinkedIn profile, or whatnot, you know, we probably don’t need to hold that information now in a classified document, right?

But there is– so, stepping through a deliberate thought process of assessing, you know, what do I have that is of value, what are my crown jewels, and then finding ways to defend it and defend it like hell, yeah, and prioritizing that over what might be more mundane or data that is already available.

[TCR 00:35:44]

**ALVARO VITTA:** That makes sense. So you’re saying in summary is, listen, identify the data, label it, classify it, categorize it, again, put some kind of risk level to it in terms of value to the organization and/or liability, right, and then, you know, govern. Put governance in place to make sure that you are able to govern the lifecycle that data throughout it’s – you know, as it goes from the enterprise and moves around everywhere that it needs to be.

**DR. MARCUS THOMPSON:** Absolutely, you know, and get it into the risk register, , get into the investment priorities, and again, trust, but verify. It’s not – this is not set and forget, because there might be something new coming up, you know, in seven seconds time that, you know, that might change our considerations here.

[25:24]

**ALVARO VITTA:**

So from your perspective, what are some practical things that government organizations can do, you know, one or two things that they can do to start on the journey, because it’s a continuous journey – it never stops, right? – that will help them optimize their data protection journey?

**DR. MARCUS THOMPSON:** The number one for mine is the labeling of data. then you can store it and it’s easier to protect and secure.

But I think also, I mean, even from a capability perspective, you know, none of us know what –what artificial intelligence technologies might come into the future. and so far, all we’re really seeing is automation rather than any – anything, sort of *Terminator*-like, you know, neurocognitive when it comes to artificial intelligence.

But irrespective of what artificial intelligence technology comes in the future, it’s going to be dependent on data. And if that data is not labeled and stored, and getting all those policies squared away now, if that data is not discoverable, that technology would be useless.

I think the other thing is, you know, because our appetite for – for digital information, for data and for electronic devices is, internationally, is insatiable. our dependence on electronic devices and digital information data is growing exponentially, you know, every day. Yeah, and I see no sign of that slowing down.

So, policies around data discoverability, you know, how long you have to keep it, so – so any wonder the construction and operation of datacenters is, you know, is such a lucrative business at the moment, certainly is in – in Australia. And obviously, yeah, Microsoft has a significant product offering in – in that regard. So, you know, hey, government, are you just going to continue to build and operate datacenters, or do you bring industry in to help you, to help you with that, whatever classification of data that – that you need for your – you know, within government?

I think they’re the sorts of things that, you know, from a pure data protection play, people can be thinking about, you know, that there’s – there’s policy aspects here. There’s technology aspects here, and there’s human behavioral aspects here.

[28:00]

ALVARO VITTA: Now, Marcus, this has been an awesome conversation. And one of the things we do in these shows is we highlight and celebrate a work of public servants from around the planet. Who’s doing that? Well, are there any examples that you have seen, either in previous lives or in the current life that you have, the current career you have, that you have seen implemented very well, that has impressed you, that has inspired you, that others can take note and say, oh wow, that’s great to hear?

**DR. MARCUS THOMPSON:** Two come immediately to mind. I mean, I have long admired what the Estonians did, you know, in terms of developing, national cyber resilience, , a comprehensive, cooperative arrangement across both government and industry, clearly led by government, you know, and clearly in response to their political, strategic, you know, circumstances there, you know, that I’m folk are all aware of. That’s the first one.

Second one, the fact that the Ukrainians are still in the fight is – is just, it’s just amazing. And And, you know, and you just look at – you just look at what national mobilization can do, and you know, a single unifying purpose with that magnificent leadership of President Zelensky. It’s impressive.

[29:30]

**ALVARO VITTA:** Thank you so much. Those are two great examples. And thank you for sharing your experiences and insights with our audience, and – and your diverse career and unique periphery of experiences. We appreciate you, and thank you so much for joining us.

**DR. MARCUS THOMPSON:** Good on you, Alvaro. I had just a great – a great time.

(Music.)

**OLIVIA NEAL:**

We hope you’ve enjoyed the second of our cybersecurity episodes. If you haven’t listened yet, I’d recommend going back and listening to our previous episode with Tom Burt. You can find this and more information on cybersecurity at wwps.microsoft.com.

Please do reach out and send us your questions and your feedback. You can find me on Twitter at @LivNeal or on LinkedIn, or you can e-mail us at ask-ps@microsoft.com Thank you and tune in next time for our third and final cyber security episode.

END