CISO LEADERS SUMMIT AUSTRALIA

International Convention Centre (ICC) Sydney

Summit Program

THURSDAY 5 OCTOBER 2017

07:45 – 08:30	**ARRIVAL & REGISTRATION**		
08:30 – 08:35	**WELCOME & INTRODUCTION** Tyron McGurgan, Chief Executive Officer, Media Corp International		
08:35 – 08:40	**MASTER OF CEREMONIES ADDRESS** Mark Sayer, Experienced Innovative Cyber Security Executive		
08:40 – 09:20	**OPENING KEYNOTE PRESENTATION (40 mins)** **Improving cyber and information security at a whole-of-government level** Dr. Maria Milosavljevic, Chief Information Security Officer, NSW Department of Finance, Services & Innovation • Protecting our information, services and assets in a holistic way • Complexities and challenges in a rapidly-evolving landscape • Changing perceptions about the role of IT versus whole of business ownership • The importance of collaboration and mutual responsibility		
09:25 – 10:05	**PANEL DISCUSSION (40 mins)** **The Price of Convenience: communications, cyber risk and cybersecurity practices of corporate boards** **Moderator:** Chris Lawley, Vice President of Sales, Diligent **Panellists:** Ajoy Ghosh, Chief Information Security Officer, icare NSW Shane Watt, Chief Information Security Officer, Newscorp Monica Schlesinger, Non Executive Director, Advisory Board Group Over the past decade, the issue of cybersecurity has increasingly gained attention in boardrooms around the world, adding yet another critical topic to already packed board agendas. Cyber risk, which has always represented a significant area of enterprise risk, is finally being acknowledged as intersecting with other areas of the board's oversight, including strategy, operations, and legal, financial, and reputational risks. Yet, while more directors now recognize that their company's cyber risk management strategy is an area of board concern, many directors lack the necessary expertise to feel fully confident in navigating cybersecurity issues. During the panel discussion, we will address the following areas: • Cybersecurity awareness begins and ends at the top – how better informed and educated board members set the tone for the entire organisation • Board communications security and oversight • The risk of e-discovery • Cybersecurity auditing and training for directors		
10:10 – 10:40	**KEYNOTE PRESENTATION (30 mins)** **Levelling-up the security status quo** Stuart Mort, Director of Cyber Security, Optus		
10:40 – 10:55	**NETWORKING BREAK**		
11:00 – 11:30	**ONE-TO-ONE MEETINGS 1**	**11:00 – 11:30**	**WORKSHOP 1 (30 mins)** **Cyber Security and Innovation: Protecting business IoT, cloud and mobile systems** Jonathan Jackson, Head of Technical Solutions & Cyber, Asia Pacific & Japan, Blackberry

			Business today needs to embrace innovative technology such as Enterprise of Things, cloud and enterprise mobility to remain competitive. But what is the price of this innovation? • In a world when cyberattacks are increasing in frequency and severity, how do you ensure your innovation and company data is protected? • How can security, cloud and mobile vendors work together to ensure systems are secure? • With increasing compliance and regulatory requirements being enforced, how can companies ready themselves for topics like GDPR and Mandatory Breach Notifications in 2018? • With employee risk to cyber security increasing on mobile devices, how should companies prepare for these threats?
11:35 – 12:05	**ONE-TO-ONE MEETINGS 2**	**11:35 – 12:05**	**WORKSHOP 2 (30 mins)** **Isosceles Security** Ben Walker, Head of Data Security, Medibank Often good security is described as a triumvirate good of Process, Technology and People. With all three elements being most critical to ensure well-rounded protection against threats, however, this presentation will describe how good Processes are irrelevant if you don't ensure that People and Technology are at the centre of good security design. The People element of cyber security is often neglected for the more "sexier" technology. However, without the right people to implement, control, program and monitor the technology it becomes prone to human complacency, malicious use or intentional or unintentional misuse. This presentation will describe how the often-depicted equilateral triangle of cyber security is outdated and that People (or Human) and Technology aspects of security are far more important than good Process to ensure adequate protection against cyber security threats, both internal and external to an organisation's boundaries. Isosceles security describes how Human Centred technology solutions will become the future of Cyber security with less import placed on Process and more direction focused on cutting edge Technology designed in consideration with human factors and resultant behaviours. This presentation is authored by Dr Tim Doyle a behavioural psychologist and adjunct lecturer at Deakin University in Melbourne, Australia and Ben Walker a cyber security practitioner and researcher from Melbourne, Australia.
12:10 – 12:40	**ONE-TO-ONE MEETINGS 3**	**12:10 – 12:40**	**WORKSHOP 3 (30 mins)** **Effecting behavioural and organisational change in cyber security** Philip Hall, Cyber Security Awareness and Intel Lead, AMP

			In today's rapidly evolving threat landscape, cyber attackers motivated by the potential to make vast amounts of money are increasingly focusing on the "human" element to circumvent technical controls and processes. Attackers use highly customised and targeted phishing emails, as well as other forms of social engineering techniques in order to gain a foot-hold into organisations big and small. It only takes one staff member to fall for an attack. Your staff are a vital part of your cyber defence strategy, and need to become cyber savvy in order to protect themselves, as well as your business. But how do you go about effecting behavioural and organisational change in cyber security? Phil Hall - AMP's Cyber Awareness & Intelligence lead will share some experiences and insights into AMP's cyber awareness journey, so that you can understand the value that cyber awareness can bring to your organisation, and embark on a cyber culture journey of your own.
12:45 – 13:55	**NETWORKING LUNCH**		
14:00 – 14:40	**KEYNOTE PRESENTATION (40 mins)** **Growing an Ecosystem** Craig Davies, Chief Executive Officer, Australian Cyber Security Growth Network Having a vibrant ecosystem is the mission of AustCyber. Doing this requires everyone to be part of how we can make a measurable difference, from education, through to research and for companies having access to solutions that solve real business problems. In this talk, I'll cover just what we're doing, and what opportunities there are for CISO's to add to the growth of this segment, including getting access to top class staff and solutions.		
14:45 – 15:15	**ONE-TO-ONE MEETINGS 4**	**14:45 – 15:15**	**WORKSHOP 4 (30 mins)** **Cloud services trust & governance** Anthony Lim, Director, Cloud Security Alliance We are embracing cloud services at a rate faster than we can think, for all the good reasons of opex, flexibility, cost, business continuity etc, despite some concerns about data security and IT governance. We look at some trust & control frameworks and standards that help us deploy cloud services yet sleep comfy at night.
15:20 – 15:50	**ONE-TO-ONE MEETINGS 5**	**15:20 – 15:50**	**WORKSHOP 5 (30 mins)** **Engaging the Board in Cyber Security** Mikhail Lopushanski, Chief Security Officer, Australian Prudential Regulation Authority For some companies, cyber security is still seen as an IT risk that needs to managed by the CIO. Detective and preventive controls should be implemented through the organisation's people with physical and technical solutions. The session discusses how to engage the Board and increase their understanding of security risks.
15:50 – 16:05	**NETWORKING BREAK**		

16:10 - 16:50	**PANEL DISCUSSION (40 mins)** **Cyber security skills gap** **Moderator:** Meena Wahi, Director, Cyber Data Risk Managers **Panellists:** Craig Davies, Chief Executive Officer, Australian Cyber Security Growth Network Apoorv Cahturvedi, Information Security Manager, Cochlear Ivana Kvesic, Information Security Head of Innovation and Culture, Australia Post Is this real or just a marketing ploy? If not, what are we doing in Government & Education to get more people interested in Security?
16:55 – 17:35	**CLOSING KEYNOTE PRESENTATION (40 mins)** **What really happened 'WannaCry'? A look at the recent Global Ransomware attacks & Data branches in Australia - including Petya** Wipul Jayawickrama, Former Head of Cyber Security, Bank of Queensland Monday 26 June 2017, the world saw a malware outbreak of an unprecedented nature. This malware outbreak which began by initially targeting Ukrainian industrial control systems, spread to Europe and other locations and to diverse industries. Commonly known as NotPetya, the malware disrupted operations and supply chains of over 2000 organisations and caused 100s of millions in damage. NotPetya used the same vulnerability and exploit mechanisms used by WannaCry ransomware, which had caused some significant damage earlier in the year. Targeting various processes and management interfaces used by Microsoft Windows, NotPetya infected local machines, extracted administrative credentials, and propagated itself to other computers on the network as did WannaCry. Due to the similarities with WannaCry, NotPetya was initially thought to be a ransomware with the threat actors behind it being driven by financial motivation. This view has since been challenged by many. Notwithstanding the motivation behind NotPetya, it continues to raise questions on how we secure our systems today. It challenges the effectiveness of our current critical cyber defences and the reasoning behind current strategies such as Defence in Depth and Cyber Kill Chain. It urges us to rethink how we approach security. In this presentation Wipul will examine the impact of recent cyber security events and propose new ways to think about cyber security in an inconstant and rapidly changing world.
17:35 – 17:40	**MASTER OF CEREMONIES CLOSE** Mark Sayer, Experienced Innovative Cyber Security Executive