Cyber Risk Meetup

Virtual Events Sponsorship

WWW.CYBERRISKMEETUP.COM

CONNECTING COMMUNITIES FROM
SINGAPORE, TOKYO, SYDNEY, MELBOURNE, BRISBANE, PERTH
MEETUP AUDIENCE EXPSOURE 2,500+

Cyber Risk Meetups are going virtual – let's face it – there's nowhere else to go!

These ever-popular events, founded by Shamane Tan, a passionate Cyber Security Advisor will remain a unique opportunity to hear from an interesting and engaging line up of CIOs, CISOs and CTOs.

Meetups have consistently attracted a loyal, local audience of between 80 – 150 people and topic ranges include cybersecurity, legal and insurance, blockchain and IoT & Robotics .

Cyber Risk Meetup has sponsor opportunities for scheduled online events with audience exposure across our meetup groups in Singapore, Tokyo, Sydney, Melbourne, Brisbane and Perth, with now the opportunity to expand further – join us on the (virtual) journey!

Cyber Risk Meetup has an exclusive media partnership with My Security Media, a dedicated industry channel for security, cybersecurity and related technology professionals.

SPECIAL SPONSORSHIP OFFER

Platinum Sponsor – $3,950 (3 max)

- Introduction Brand Recognition Branding with virtual event
- 15sec Slide (content of choice) or 30 second video
- PLUS MySecurity Media Digital Promotion Package & Podcast

Gold Sponsor – $1,950 (5 max)

- Shout out in Introduction
- Closing Slide Deck – 10sec slide of choice

*All prices shown are in AUD. For Australian customers, all prices are exclusive of GST (10%) which will be added at the time of invoice.

CYBER RISKERS

Cyber Risk Meetup

Sponsor & Media Package

VIRTUAL - ANNUAL MEETUP PACKAGE 2020

CYBER RISKERS

Media Partners

MYSECURITY MEDIA APP

MYSECURITY MARKETPLACE

SINGAPORE, TOKYO, SYDNEY, MELBOURNE, BRISBANE, PERTH

Cyber Risk Meetups provide attendees a special experience and additional takeaways, including door prizes and special publications. These ever increasingly popular events were founded by Shamane Tan, a passionate Cyber Security Advisor who has a unique skill in formulating an interesting and engaging line up of CIOs, CISOs and CTOs.

Events consistently attract a loyal audience of between 80 – 150 people and topic ranges include cybersecurity, legal and insurance, blockchain and IoT & Robotic events, along with opportunity to promote specialised workshops and round-tables.

Cyber Risk Meetup has an exclusive media partnership with My Security Media, a dedicated industry channel for security, cybersecurity and related technology professionals. Cyber Risk Meetup has sponsor opportunities for scheduled events in Singapore, Tokyo, Sydney, Melbourne, Brisbane and Perth, with calls to expand further – join us on the journey!

"It's said that a wise person learns from his mistakes. A wiser one learns from others' mistakes. But the wisest person of all learns from others's successes." John C. Maxwell

Shamane Tan, Founder

I started the Cyber Risk Meetup in Sydney in 2017 with the intention to create a platform where talented people can share their experiences and key learns. Hence, I wanted to build a community where like-minded professionals can network with one another.

Passionate about these two words: **Cyber & Risk?**

Why Sponsor a Cyber Risk Meetup?

Passionate about these two words: **Cyber & Risk?**

We meet up once every quarter and start off first with networking over complimentary food and drinks courtesy of our Cyber Risk Meetup sponsors

WWW.CYBERRISKMEETUP.COM

Meeting our Cyber Riskers

550+	50+	950+	450+	100+	200+
SINGAPORE	TOKYO	SYDNEY	MELBOURNE	BRISBANE	PERTH

Cyber Risk Meetup

The future of innovation & the BIG CISO question?

Cyber Risk Meetup – Sydney Wrapup

In support of ISACA's SheLeadsTech initiative and once again, months of hard work, the Cyber Risk Meetup moved on from a successful Singapore meetup and back to Sydney. At the central high-rise offices of AWS, and sponsored further by Privasec, nearly 150 cyber riskers heard from six special guests in an exclusive two segment panel session.

The Future of Innovation panel, moderated by Igor Shparberg, Director, e-Pocket (Int) and joined by Gillian Findlay, COO, Safety Culture, Frances Bouzo, Head of IT Security, iCare NSW, and Tabitha Bauer Executive Manager of Digital Assurance, CBA kicked off with 'What gets you up in the morning?' The panel entered a great discussion, from finding offices for a start-up in Surry Hills, motivating young people, and through to building a commercial minded enterprise but that also makes people feel better. The things we see in cyber security is continually challenging and changing, so it is self-motivating, but with young kids, the alarm clock still helps!

'How do you keep up and translate it day to day?' – "I hire people who are smarter than me", said one panellist. Look at what's coming. Put in automation and have a mix of people – the questions asked often creates learning and then technically trying to continually improve and set the bar high in cybersecurity.

How important is diversity? In Australia we should do more with it and use it to our advantage, far more so as we work and think globally – in a global industry with global resources. Recruiting on aptitude rather than qualifications is also an important factor, particularly in cybersecurity. Interestingly, but maybe not surprisingly, 'return to work mothers' and 'military veterans' have both been shown to show positive aptitude for cybersecurity. Maybe it's the 'battleground' traits they share?

The younger generation are doing so much more with technology and the expectation on younger people will continue to be so much more. However, the digital disruption is only just beginning. The way we recruit is still using tunnel vision and we can learn a lot of lessons from the past – a good example is how start-ups can be a source of learning for large enterprise and likewise start-ups can learn from enterprise on how to scale. One good takeaway line was "We don't have to reinvent, but we have to catch up!"

The second panel, 'Where do I put my CISOs? moderated by Cyber Risk Meetup organiser Shamane Tan, APAC Cyber Security Advisor, Privasec was joined by Robert Lang, CTO, OpenMarkets, Stuart Mort, CTO – Cyber Security, Optus Business and Wouter Veugelen, CISO, Primary Healthcare. Matching the variety of the panel, was a variety of responses.

> 'With a packed room and nearly 100 on a waiting list, this Cyber Risk Meetup was well served with great content, a fascinating networking mix, as well as great food and drink.'

CISO's should be their own line of business, was one view, though in contrast one panellist reported to the CIO. How to get cybersecurity embedded into the enterprise is a well-recognised challenge. Too often plans are put in place after the breach has occurred. Reporting to the CIO is okay but CISOs may still be segregated to have policy freedom and separate to operations. Organisation size and maturity all has an influence on where the CISO may sit.

What skills does a good CISO have? Paranoia is good! Anticipating the unexpected, being able to adapt the language to stakeholders, be across the C-Suite. Cybersecurity can be perceived as complex – trying to use analogies can help, such as brakes on a car are there for safety but allows the car to drive faster. CISOs also need to understand the business and the biggest hurdle can often be the sales team – who and what is really driving the business. Security should enable the business and be engaged.

Dealing with a breach is about learning – and learning fast – is it a technical, people or process fail and then getting all the ducks in a row for communications, legal and executive. If it's a failure in the risk assessment then the CISO hasn't done their job.

With a packed room and nearly 100 on a waiting list, this Cyber Risk Meetup was well served with great content, a fascinating networking mix, as well as great food and drink.

If you are looking for an event of quality networking and new connections, or you just want to see what's the Cyber Risk hype all about – visit www.cyberiskmeetup.com and stay tuned for your next complimentary meetup.

BTW – ARE YOU A POTENTIAL SPONSOR? Chat to Shamane Tan or Chris Cubbage about how you can get exposed in a multi-media package for event and media exposure in Australia and Singapore.

SPEAKER PROFILES

Gillian Findlay is the Chief Operating Officer of SafetyCulture, the creators of the world's most used safety and quality inspection app, iAuditor and recently launched real-time incident reporting tool, Spotlight. The company currently employs over 220 people in five offices around the world, and recently raised $60M in Series C funding. With over 15 years experience in finance, strategy and operations, Gill is instrumental in navigating the challenges that face a global technology start-up experiencing rapid growth. Prior to working at SafetyCulture, Gill worked in top tier consulting and ASX listed companies.

Frances Bouzo is the Head of IT Security and Risk at icare a provider of insurance and care services to people with injuries under the NSW state government insurance and care scheme. icare delivers insurance and care services to the businesses, people and communities of NSW and is one of the largest insurance providers in Australia. Frances has over 23 years' experience in information technology with eleven of those specialising in information security and technology risk. Prior to joining icare, Frances held various leadership roles including Global Director Security Risk and Controls at Aon a global provider of risk, retirement and health solutions and IT Security & Operations Manager at Employers Mutual an injury management partner for employers and government agencies. During her tenure at Employers Mutual Frances led the information security program, taking the organisation through the ISO27001 certification process enabling Employers Mutual to achieve and maintain certification. Frances holds a Masters of Management Information Technology and various technology and security certifications including Certified Systems Security Professional (CISSP) and ISO27001 Lead Auditor.

Tabitha Bauer grew up with computers when they had no hard drives and when Battlechess was the coolest game to play! Coding since she was 10, Tabitha has grown up with computers and has followed the industry's rapid evolution with great enthusiasm. With a strong academic background in networking and artificial intelligence, Tabitha has spent the majority of her career as a Computer Forensic consultant where she investigated the technology aspects of criminal and civil cases in support of law enforcement, regulatory bodies and top-tier law firms. Currently she leads a very talented Digital Assurance team who provide white-hat hacker security testing and application security consulting within the Commonwealth Bank. Tabitha is passionate about educating and supporting young people who want a career in cyber security and works with partnering universities to provide industry relevant teaching material and real-world work experience opportunities.

Igor Shparberg is the Director of e-Pocket, an advanced platform that delivers a sophisticated payment solution. He is an experienced & highly motivated professional with broad experience across banking & broker distribution sales, strategy, capability development, customer and relationship management. With a strong focus on innovation of sales and service channels, his experience in leadership & coaching of diverse teams has seen him developing as an entrepreneur who enjoys the challenge of developing new products with a view of benefiting the society.

Wouter Veugelen is a Chief Information Security Officer with 15+ years of professional experience in technology and cyber security. His industry experience spans different sectors including Financial Services, Health, and Energy, Utilities and Mining sectors both in industry roles as well as within professional services roles.

Robert Lang is the CTO of OpenMarkets, a digital trading platform that provides retail investors, traders, advisers, robo-advisers, brokers and financial intermediaries with a suite of innovative brokerage services for trading on the Australian securities markets.

Previously he was CEO of Auggd, a market leading startup in AR/VR products and services. From 2007-2013, Rob led the technology and software development for all SMARTS products as CTO, including managing the technology transition to Nasdaq when SMARTS was acquired in 2010. From 2013 through 2016, Rob lead the SMARTS and TradeGuard businesses inside Nasdaq and was GM of the Nasdaq Australia office. Prior to 2007, Rob spent 10 years in various technology management roles mostly in Silicon Valley, California, producing hardware products in the computer graphics and image processing industry, most notably for Silicon Graphics and Nvidia. Rob received a PhD in Computer Engineering from Newcastle University in Australia in 1996 and he is an independent Board member of the Capital Markets Cooperative Research Centre (CMCRC).

Stuart Mort has 25 years of experience working in Security, from Special Duties operational work with the British Government through to heading an international security consultancy team, and then spending 12 years as Oracle's Global Vice President of Information Security, a CISO role with the group reporting independently to President-level with full cross-corporate oversight; a fully independent Line of Business and not a sub-set of a technology team. As Optus's CTO Cyber Security, Stuart brings extensive experience to help Optus partner with our customers as a subject matter expert, trusted advisor and thought leader to aid in addressing the security threats of today and tomorrow. As well as being a keen triathlete, having represented Australia at Age Group Level at the World Championships, Stuart is a Full Member of the Institute of Information Security Professionals, holds a Master of Laws and has served as an Expert Witness in a variety of Court cases.

Shamane Tan is the Cyber Security Advisor at Privasec, a premium Australian Security Consulting Firm and PCI QSA Company. In her previous roles, she has worked with exciting start-ups all the way to global organisations extensively across Singapore, Malaysia, and Australia. Shamane advises the C-Suite and IT Executives on the reality of the challenges they faced from the regulatory issues to cybercrime. This led her to take up this APAC role with Privasec and provide advice to businesses on uplifting their Security posture. Shamane has a passion for disruptive technologies and human factor and is the founder of the Cyber Risk meetups across Sydney, Melbourne and Singapore. The meetups offer Security Enthusiasts and Executives a unique platform to impart and exchange innovative insights. As member of the Australian Women in Security Network (AWSN), Shamane is also a huge advocate and champion for women in IT Security and is keen to encourage more people to take the step forward in the world of Cyber.

Cyber Risk Meetup

Cyber Risk meetup launched in Singapore

It was indeed a very special and exclusive evening in Singapore last night where nearly 70 guests were gathered and treated to the insights of industry experts, including an APAC Chief Technology Officer, Chief Information Security Officer and APAC Head of Security Intelligence, as well as Ted-talk style presentations on 'Phishing versus Vishing' and artificial intelligence and how Cyber is evolving with it.

With thanks to the venue host, JustCo, the meetup kicked off with a panel discussion addressing the impact of Singapore's Cyber Security Act and the key regional trends being observed. Cyber Risk Meetup Organiser Shamane Tan was joined by Ian Yip, APAC CTO at McAfee, Ricardo Gonçalves, APAC Head of Security Intelligence at Barclays Group and Prashant Haldankar, Co-founder at Privasec, now operating in Singapore. Ricardo gave particular guidance on what all businesses need to be doing, particularly given the third party risks that supply chains carry in cyber environments – it is not just the big end of town taking the threat seriously – the larger enterprises are now making their suppliers accountable. Also an extra warning to cryptocurrency traders to take special care with crypto-currencies and exchanges under sustained and sophisticated attack.

Noordin, CISO at NTUC Link delivered an entertaining Ted-Talk Session 'Are You Feeding The Phish?' Getting an awareness campaign into an enterprise is no easy task, however Noordin's presentation showed it can be done, as well as the grave importance on getting staff and stakeholders to STOP clicking on those links and worse – freely giving out their credentials!

And to top off a great night of food, drinks and networking, the charming Charles Crouspeyre, Head of Accenture's Artificial Intelligence ASEAN practice gave an eye-opening presentation on where AI is and likely to be taking us with his Ted-Talk Session 'Cyber Security & AI: A New Paradigm?' – hang on to your hats folks – AI is taking us to a realm of making the unreal appear real – Fake News is just the start of where we are likely to be heading.

Congratulations to Ms Yuk Lin for winning the evening's door prize, a free conference pass to the RSA APJ Conference 25 – 27 July in Singapore – Yuk worked hard to win by being the most active Tweeter for the night #cyberriskmeetup – Congratulations Yuk! And thanks for the great and to quote "awesome" feedback!

Finally – a special thanks for the Platinum Sponsor – McAfee. We sat down with Ian Yip today to capture Ian's insights to share further – Stay tuned on the Cyber Security Weekly Podcast

Speaker Profiles:

Ian Yip has worked with organisations globally on Cyber Security initiatives and projects. He has held a variety of leadership roles across Europe and Asia Pacific in some of the world's leading companies, including McAfee, Ernst & Young, IBM, CA Technologies and NetIQ. In addition to being a published author, Ian has built, led and managed teams with multi-million dollar sales, delivered major cyber transformation programs & engagements, delivered keynote presentations at industry & corporate events, been interviewed & quoted in the media.

Chris Cubbage, MySecurity Media welcoming Cyber Riskers

Ricardo Gonçalves joined Barclays in 2017 to head their APAC security intelligence efforts. Before that, Ricardo worked for the last 3.5 years with Commonwealth Bank of Australia shaping the internal cyber intelligence function and working next to the IR and CyberCrime teams. His tasks would range from executive communication to dissecting malware web-injects. A key aspect of his role was the creation of a solid (and fruitful) network between law enforcement, industry peers, and internal business stakeholders. Outside of work, Ricardo likes to contribute back to the community by volunteering his time to security-focused not-for-profit organisations.

Prashant Haldankar is a Co-Founder at Privasec which is an independent security consulting firm. He gained extensive IT security experience within Australia and internationally and overall has over 15 years of experience in information technology and information security. He has worked in various roles in Australia and overseas, in Senior positions for government, private sectors and consultancy firms to establish and implement information security strategies and frameworks. He has planned, managed and developed security assessment and audit methodology in Australia and internationally to achieve security compliance objectives for global organisations. He is also a Payment Card Industry Data Security Standard Qualified Security Assessor (PCI QSA) and has successfully assisted many merchant organisations and service providers to achieve and maintain PCI DSS compliance.

Shamane Tan is the Cyber Security Advisor at Privasec, a premium Australian Security Consulting Firm and PCI QSA Company. In her previous roles, she has worked with exciting start-ups all the way to global organisations extensively across Singapore, Malaysia, and Australia. Shamane advises the C-Suite and IT Executives on the reality of the challenges they faced from the regulatory issues to cybercrime. This led her to take up this APAC role with Privasec and provide advice to businesses on uplifting their Security posture. Shamane has a passion for disruptive technologies and human factor and is the founder of the Cyber Risk meetups across Sydney, Melbourne and Singapore. The meetups offer Security Enthusiasts and Executives a unique platform to impart and exchange innovative insights. As member of the Australian Women in Security Network (AWSN), Shamane is also a huge advocate and champion for women in IT Security and is keen to encourage more people to take the step forward in the world of Cyber.

Mohamed Noordin has over 16 years of experience in diverse roles ranging from Cybersecurity, IT/Operational Audits, Compliance, Investigations and Forensics. He started his career with the Singapore Police Force (SPF) and then worked in companies such as Ernst & Young and Barclays. He took up a role after as an expatriate with an oil and gas company in the middle east to help set up and formalise the Special Investigations team, which later became the Ethics & Compliance section within the Internal Audit department. Noordin came back to Singapore as an Associate Director with the Cybersecurity team in KPMG where he led cybersecurity services for the government sector and was also the privacy service line lead. He also headed the internal IT Security team as Deputy CISO and DPO in KPMG Singapore and its regional offices. At the start of 2018, he took up a role to head cybersecurity and infrastructure in NTUC Link, and concurrently leads the Cybersecurity Centre of Excellence (CoE) function in NTUC Enterprise across the group. Noordin is also the co-founder of PhishNow – a SaaS and subscription-based Phishing Simulator.

Charles Crouspeyre has 11 years of experience in the Artificial Intelligence field where he has successfully implemented Machine Learning solutions across multiple industries: Homeland Security & Military, Fintech, Advertisement etc. Charles has been living in South East Asia for the last 6 years where he has created 2 startups (one focused on predictive maintenance for the Oil & Gas industry – in Singapore and Indonesia, one on fraud detection and credit scoring for unbanked populations – in Singapore and Philippines). Prior to joining Accenture, he was leading the Innovation Centre of a multinational Advertisement company.

Privasec is a leading provider of Cyber Security Services to Government, Financial Services, Retail, IT, Health, Entertainment and Not-for-Profit sectors. Privasec GRC are the specialists in Governance, Risk and Compliance including ISO 27001, IRAP Assessments and PCI DSS. Privasec RED are leaders in Red Team Attack simulations, Physical Intrusions, Theft simulations, Open Source Intelligence Gathering (OSINT), Social Engineering, Phishing and Drone Security. We believe in partnering with our customers and building long-lasting relationships, integrity and care. We build our success on trust and are completely vendor agnostic. We hold numerous accreditation and are ISO27001:2013 certified. With offices in Sydney, Melbourne, Brisbane and Auckland, we are on several State and Federal Government panels.

JustCo is Singapore's largest co-working space in the Central Business District (CBD). JustCo was established to meet the growing demand for creative, collaborative workspaces integrating lifestyle, community and technology into the work environment. It offers an open and dynamic environment which includes an expansive common area for networking and collaboration, as well as a games room for clients to relax and unwind. Clients have the flexibility of getting a desk or a dedicated and secured studio space with access to all shared facilities.

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. For businesses, McAfee helps orchestrate holistic cybersecurity environments that work smarter, not harder. For consumers, McAfee helps by securing their digital lifestyle at home and away.

MYSECURITY MEDIA

MYSECURITY MARKETPLACE

MYSECURITY MEDIA

Download on iTunes | GET IT ON Google Play

Bringing all of the MSM channels together on one platform for the latest and greatest in security, technology and events from across the Asia Pacific and the world. Now available on Apple and Android platforms.

Cyber Security WEEKLY PODCAST

The Cyber Security Weekly Podcast has surpassed 180 interviews and provides regularly updates, news, trends and events. Over **200,000** downloads and 2,500+ downloads an episode.

CYBER RISK LEADERS

A dedicated channel for Boards, C-Suite Executives and Cyber Risk Leaders to highlight cyber threats as a key business issue.

CYBER RISKERS

EXCLUSIVE MEDIA PARTNERS

Event opportunities in Sydney, Melbourne, Brisbane & Singapore providing attendees a special experience and additional takeaways, including podcast interviews and print media. Visit **www.cyberriskmeetup.com**

AUSTRALIAN CYBERSECURITY MAGAZINE

The Australian Cyber Security Magazine was launched in agreement with the Australian Information Security Association (AISA) to be focused on AISA's 3,000 members, nationally and forms part of AISA's national cyber security awareness and membership communication platform.

AUSTRALIAN SECURITY MAGAZINE

The Australian Security Magazine is the country's leading government and corporate security magazine. It is published bi-monthly and is distributed to many of the biggest decision makers in the security industry. Provoking editorial and up-to-date news, trends and events for all security professionals.

ASEAN Tech&Sec www.aseantechsec.com

The region's newest government and corporate Technology and Security magazine, with a focus on the Southeast Asia region and the 10 ASEAN member nations

APSM ASIA PACIFIC SECURITY MAGAZINE

My Security Media rapidly expanded into the Asia Pacific Region with its sister publication – the Asia Pacific Security Magazine. It is published bi-monthly. It is available online to read by all and upon every issue release a direct link is sent to a database of subscribers who are industry decision makers.

Drones & Robotics DRASTIC news.com

Dedicated channel for all things about Drones, Robotics, Autonomous systems, Technology, Information and Communications

CHIEF IT TECHNOLOGY CHANNEL PARTNERS www.chiefIT.me

Technology channel partner ecosystem platform with a natural focus on Big Data, Internet of Things and fast emerging technologies

MYSECURITY ROUNDTABLES

MySecurity Media can facilitate specialist round-table luncheons or breakfast sessions for up to 20 invited guests for high level discussion on Security & Cybersecurity themes, guided by the Vendor's Leaders and accompanied with published content.

MySecurity TV

The MySecurity TV Channel delivers news and interviews for the Asia Pacific Security Magazine, Australian Security Magazine and Australian Cyber Security Magazine – and from across MySecurity Media channels.

promoteme@mysecuritymedia.com
www.mysecuritymedia.com

THE 'GO-TO' TOOL FOR LEADING PROFESSIONALS

MYSECURITY MARKETPLACE

SCAN ME

- ✓ UP COMING EVENTS
- ✓ COURSES
- ✓ WEBINARS
- ✓ WHITEPAPERS
- ✓ SOFTWARE

promoteme@mysecuritymedia.com
www.mysecuritymarketplace.com

AUSTRALIAN CYBERSECURITY MAGAZINE

Cyber Security WEEKLY PODCAST

Download on iTunes

GET IT ON Google Play

PODCAST HIGHLIGHT EPISODES

Cyber Security WEEKLY PODCAST

Episode 73 – Tech convergence - Drones, 3D printing & payloads – Nigel Brown, Autonomous Technology

Nigel Brown, Director of Autonomous Technology provides insights into running a certified drone operation, with a particular focus on the mining and resources sector in Western Australia. As a recent client of Konica Minolta's 3D printing technology, Nigel Brown provides discussion on the application of 3D printed parts and payloads and how the application of fast-developing 3D printer systems provides new business opportunities with developing smaller and lighter payloads.

Episode 67 – Tech & terrorists, drones & devices – insights from australia's leading terrorism researcher – Professor Clive Williams, ANU

Professor Clive Williams, Centre for Security and Military Law at the Australian National University has been a staple provider of research into national security and counter terrorism for many years. Professor Williams provides current insight into terrorism activity in the Asia Pacific, including the Marawi seige in 2017 where 1,000 insurgents were killed, and provides a chilling warning which rang true about Islamic State fighters returning to their homeland and posing a threat. Bombings in Surabaya, Indonesia two weeks (13 May) after this warning proved him correct.

Episode 71 – Tech-crime & international policing 2.0 - Europol's former executive director Rob Wainwright

Technology has transformed a whole range of different crimes and new avenues for terrorists to explore, including exploitation of social media platforms, as seen by the Islamic State. We are always racing against criminals to a certain extent but have great potential on the policing side.

Rob Wainwright, former Executive Director at Europol, gave an earlier presentation at Cebit Australia. His presentation, 'Data – the new oil in the network economy fighting crime and terrorism', highlighted a different age to come. Rob termed this 'International Policing 2.0', along with the AI race with crime, security by design and privacy by design.

Episode 62 – Austcyber's knowledge priorities - interview with Mike Bareja, Program Manager - National Network

In this interview, Morry Morgan speaks with Mike Bareja, Program Manager - National Network at AustCyber - The Australian Cyber Security Growth Network Ltd following his presentation at CIVSEC 2018 in Melbourne.

Mike outlines AustCyber's Cyber Security Sector Competitiveness Plan and the 5 DARPA Grand Challenges or Knowledge Priorities, where resources and attention are focused on:

- Emerging prevention, detection and response technologies;
- dentity, authentication and authorisation in the cyber domain;
- Ensuring security, privacy, trust and ethical use of emerging technologies and services; and
- Approaches to deal with the increasingly 'shared' responsibility of cyber security.

Funding of $15M over 4 years is available for industry-led, collaborative projects that address the key issues from the Industry Knowledge Priorities.
Media independently of the Risk Management Institute's National Conference.
Recorded November 16, 2017, Canberra.

Episode 69 – Moving the dial: Measuring the relationship between the user and their activity on a machine: Interview with Jeff Paine, CEO & Founder, ResponSight

Jeff Paine, CEO and Founder of ResponSight, a three year old Australian start-up that elevates enterprises away from focusing on technology alone, discusses the link between the technology and user. Statistical and telemetry based, ResonSight has a lightweight footprint in its risk analytics and risk profiling outcomes that help enterprises make decisions.

Chris and Jeff talk about the three key components, the ResponSight Collector, ResponSight Aggregator and ResponSight Cloud Service, each working in conjunction. By combining large volumes of raw numerical telemetry and selected metrics, it's possible to build activity and behaviour profiles about users and their devices, without ever knowing who that user is or what that device is. This also provides the ability to profile the organisation's risk at a point in time, and over time. The design philosophy is to not collect private or sensitive data. There isn't a need for rich and potentially sensitive data for security.

Episode 60 – The fundamentals of operating a secure cloud, Rupert Taylor-Price, CEO of Vault Systems

In this interview, Chris Cubbage talks to Rupert Taylor-Price, Founder and CEO of Vault Systems, an Australian-owned, sovereign cloud provider, for highly protected data, purpose built for the Australian government.

Created to enable multiple departments share cyber security infrastructure, Vault Systems have moved into a mainstream government cloud platform, in part by the 2014 cloud-first initiative. Since then, Vault, which was founded by Rupert, has smashed expectations, and recently secured the biggest cloud deal in the history of the Australian government.

www.australiancybersecuritymagazine.com.au

Cybersecurity in-depth in APAC

Ian Yip, APAC CTO at McAfee

In this episode we are joined in Singapore by Ian Yip, APAC CTO at McAfee and discuss the impact of Singapore's Cyber Security Act and the key regional trends being observed. We also discuss the business structure and scale of McAfee and dive into McAfee's latest Threat Report, June 2018 with highlights around the latest cyber campaigns – Gold Dragon Expands the Reach of Olympics Attacks: Lazarus Rises Again, Targeting Cryptocurrency Users; and Advanced Data-Stealing Implants GhostSecret and Bankshot Have Global Reach and Implications.

Ian also provides valuable advice as to the vulnerabilities of blockchain technology and concludes with insight into communicating to the Enterprise C-Suite and an upcoming McAfee whitepaper.

Also in recent news, McAfee's Advanced Threat Research team have revealed in an investigation into underground hacker marketplaces, a major international airport's security system (including building security automation) for sale on the dark web via a Russian 'RDP shop'. The asking price: just $10.

Remote Desktop Protocol (RDP) is a proprietary Microsoft protocol that enables remote administrator access to a PC, something great for solving IT challenges, but potentially devastating if in the wrong hands. In this instance, any hacker wanting to gain control of the airport's system only needed a few dollars to access to a compromised machine and potentially carry out a myriad of large-scale attacks that could have severe consequences for the airport and its customers. For example, RDP can be used as an entry point to send spam, create false security alerts, steal data, credentials and even mine cryptocurrency. As we saw with the recent SamSam ransomware campaign against several US institutions, RDP was used to enact the attack and claim ransoms as high as $40k.

Recent trends in dark web marketplaces are also outlined in the research. One key finding is that RDP shops are growing in their size and abundance on the dark web – ranging from 15 to more than 40,000 RDP connections for sale at Ultimate Anonymity Service (UAS), a Russian business and the largest active shop they researched.

You can find further details of the attack in McAfee's latest blog post.


Ian Yip, APAC CTO at McAfee

Cyber Security WEEKLY PODCAST

AUSTRALIA
Cyber Risk Meetups
Media Supporter Package

Passionate about these two words: **Cyber & Risk?**

The Cyber Risk Meetup has event opportunities in Sydney, Melbourne & Singapore and will provide attendees a special experience and additional takeaways, including the Australian Security Magazine.

Shamane Tan, organiser of the ever increasingly popular Cyber Risk Meetup events in Sydney and Melbourne, has partnered with MySecurity Media for an exclusive media partnership. Shamane Tan is a passionate Cyber Security Advisor and MySecurity Media is a dedicated industry channel across the Asia Pacific for security, cybersecurity and related technologies.

Events attract a loyal audience of between 80 – 150 people and topic ranges include cybersecurity, legal & insurance, blockchain and IoT events, along with promotion of specialised workshops and round-tables.

CYBER RISKERS

Bronze	$2,500	• Logo on slides for Online event • Logo displayed on the Cyber Risk Meetup website. • Brand awareness shoutout by the Online event facilitator • Sponsorship logo on the MySecurity Marketplace website
Gold	$4,000	• Logo on slides at Online event • Logo on the Cyber Risk Meetup website • Brand awareness shoutout by the Online event facilitator • Podcast interview on The Cyber Security Weekly Podcast • 4 weeks - logo on Australian Cyber Security Magazine website • Sponsorship logo on the MySecurity Marketplace website
Platinum	$5,500	• Logo on slides at Online event • Logo on Cyber Risk Meetup Event website • Brand awareness shoutout by the Online event facilitator • Featured individual podcast interview on The Cyber Security Weekly Podcast • 4 weeks - logo on Australian Cyber Security Magazine website • Sponsorship logo on the MySecurity Marketplace website

All prices are plus GST which will be added at time of invoice.

Join us at an event | Register at **www.cyberriskmeetup.com**
Support an event | Register at **promoteme@mysecuritymedia.com** or visit **www.mysecuritymedia.com**

SINGAPORE & JAPAN
Cyber Risk Meetups
Media Supporter Package

Passionate about these two words: **Cyber & Risk?**

CYBER RISKERS

The Cyber Risk Meetup has event opportunities in Singapore, Sydney, Melbourne & Brisbane and will provide attendees a special experience and additional takeaways, including the Australian Security Magazine.

The ever increasingly popular Cyber Risk Meetup was founded by Shamane Tan, a passionate Cyber Security Advisor. The Meetup has an exclusive media partnership with My Security Media, a dedicated industry channel across Asia Pacific for security, cybersecurity and related technologies.

Events attract a loyal audience of between 80 – 150 people and topic ranges include cybersecurity, legal & insurance, blockchain and IoT events, along with promotion of specialised workshops and round-tables.

Bronze	SG$2,500* US$2,500*	• Logo on slides at Online event • Logo displayed on the Cyber Risk Meetup website. • Brand awareness shoutout by the Online event facilitator • Sponsorship logo in the MySecurity Marketplace website
Gold	SG$4,000* US$4,000*	• Logo on slides at event • Logo on the Cyber Risk Meetup Event website • Brand awareness shoutout by the event facilitator • Podcast interview on The Cyber Security Weekly Podcast • 4 weeks - logo on Asia Pacific Security Magazine & ASEANtechsec.com website • Sponsorship logo on the MySecurity Marketplace website
Platinum	SG$5,500* US$5,500*	• Logo on slides at event • Logo on Cyber Risk Meetup website • Brand awareness shoutout by the event facilitator • Featured individual podcast interview on The Cyber Security Weekly Podcast • 4 weeks - logo on Asia Pacific Security Magazine & ASEANtechsec.com website • Sponsorship logo on the MySecurity Marketplace website

**All prices are exclusive of Singapore taxes which will be added at time of invoice. USD charged for Tokyo events.*

Join us at an event | Register at **www.cyberriskmeetup.com**
Support an event | Register at **promoteme@mysecuritymedia.com** or visit **www.mysecuritymedia.com**

Speaker hall of fame

LEARNING FROM LEADING CISOS, CTOS, CIOS & CEOS

Hank Opdam
CISO,
Star Entertainment Group

Hai Tran
CISO,
WA Police

Wouter Veugelen
CISO,
Primary Healthcare

George Arronis
CISO,
Serco Australia

Ben Chung
CISO,
NTT ICT

Prashant Haldankar
CISO,
Privasec

Mohamed Noordin
CISO,
NTUC Link

Lisa Giacomelli
CRO,
YMCA

André Jenkins
CIO,
NSW Health Agency

Gillian Findlay
COO,
Safety Culture

Stuart Mort
CTO - Cybersecurity,
Optus Business

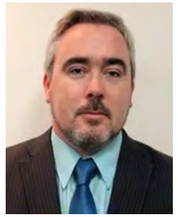
Hank Opdam
CTO,
OpenMarkets

Ian Yip
APAC CTO,
McAfee

Ricardo Gonçalves
APAC Head of Security
Intelligence,
Barclays Group

Patrick Gunning
Law Partner
King & Wood Mallesons

Tabitha Bauer
EM of Digital Assurance,
CBA



Trevor Cushen
Head of Information Security,
BPAY

Frances Bouzo
Head of IT Security,
icare NSW

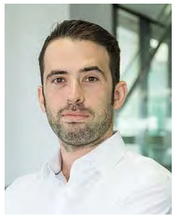
Dr. Timothy Doyle
Principal Psychologist,
Proof of Character

Fergus Brooks
Cyber Risk National
Practice Manager,
Aon Australia

Meena Wahi
Director,
Cyber Data-Risk Managers

Daryl Chew
Regional Information Security
Head (APAC),
Anglo American

Matt Tett
Chair of IoT Alliance Australia
Work Stream 5



HaCharles Crouspeyre
Head of ASEAN Artificial
Intelligence, Accenture

Ted Ringrose
Partner,
Ringrose Siganto

Tony Vizza
Director of Cybersecurity
Advocacy, APAC, (ISC)^2

Manan Qureshi
APAC Head of Security
Strategy, IBM
CYBER RISKERS

Tony Jarvis
Chief Strategist
- APAC, Middle East & Africa
Check Point Software
Technologies

Cyber Risk Meetup

Interview with **Shamane Tan,** the Founder of Cyber Risk Meetup

2018 has been an incredibly rich year, packed with conferences and events as the Cyber Security industry tries to keep up with trends and governance. In the midst of all that, there was a meetup group that stood out amongst all other meetups and very quickly became known as a class of its own. It was the Cyber Risk Meetup, which has rapidly become a well-known favourite and one of those NEED TO ATTEND event.

We interviewed Shamane Tan, the Founder of Cyber Risk Meetup on its uniqueness. As the APAC Head of Cyber Risk Advisory with Privasec, a leading Cyber Security consulting firm, she also works with her GRC and Technical Assurance team together with the different CISOs to bridge security gaps in organisations.

Q: Why do you do what you do?

In my last 9 years in this industry, if it's one thing I learnt - is that people are our biggest wealth when it comes to experience. If we are patient enough, there is so much that we can draw from their deep wells of knowledge. I started the Cyber Risk Meetup in Sydney in 2017 with the intention to create a platform where talented people can share their experiences and key learns. 'It's said that a wise person learns from his mistakes. A wiser one learns from others' mistakes. But the wisest person of all learns from others's successes.' Hence, I wanted to build a community where like-minded professionals can network with one another. In doing so, I find out their actual challenges, and was inspired to organise my events around topics that industry leaders are so passionate about! I never expected it to scale up the way it did.

Q. How does it work?

We meet up once every quarter and start off first with networking over complimentary food and drinks courtesy of our Cyber Risk Meetup sponsors. (Shout out to Privasec for being our biggest supporter and for all their active contributions to the different industry events.) After a period of time, even strangers will become a friendly face and it helps to speak to a peer or one of the executives in the same industry. I was recently watching Ocean's Eight on the plane and it's interesting to see how the bad girls had to collaborate together to pull off the biggest steal of the century. How much more do we need to work together and be more active in sharing our ideas as we battle together to protect our loved ones and workforce in this digital age. The meetups provide a fantastic opportunity for professionals, our new generation and the general public to come together and learn from one another in a comfortable and safe environment. Indeed it takes a community to build a community.

Q. Share your vision for the Cyber Risk Meetups

We are vendor agnostic and extremely big on encouraging new faces and voices in this industry. Our Cyber Riskers (that's what we call our members) get to hear from renowned industry speakers that they do see at conferences but also get to hear from fresh new speakers. Most of them being a CISO have had extensive experience leading people but somehow had never put their hands up to speak. Imagine my great delight several of our Cyber Risk speakers were discovered through our events and now speaks at major national conferences.

Q. What was 2018 like?

It was incredibly exciting. We are at 800 members in Sydney, and already at 400 members in Melbourne with our inaugural launch just early March this year. Cyber Risk Meetup saw a successful launch in Singapore in July and was closely followed by Brisbane this September. We have now crossed over the 1,500 members mark across Australasia. We are always oversubscribed and full house with more than 100 attendees turning up each time.

Q. Can you share some of Cyber Risk Meetup's highlights?

What I love about our meetups is that they are all so diverse. One moment I am in Melbourne hosting presentations on the evolution of Artificial Intelligence, and the next session, I am moderating C-suite discussion panels on CISO matters in Sydney. There was a really memorable session we organised around Data Privacy where we had two law partners taking opposite sides at a debate on GDPR and the impact of the NDB's amendment. At another of our meetups, we had a clinical psychologist present on the human factor and the insider threat. Singapore also saw a mini Ted-Talk style Cyber series and we had various ASEAN Heads and CISOs exposing the secrets of the Hacker all the way to presenting on Machine Learning.

Q. What does the future look like for the Cyber Risk Meetups?

We are very excited to launch Cyber Risk Meetup in Perth on the 19th of November, as part of WA Cyber Week as part of the WA AISA Cyber week. Also, for the first time ever, Cyber Risk Meetup will be running our very own Summit as a joint event with Privasec in Feb 2019.

Do stay tuned for more details! Cyber Riskers can subscribe to the events at cyberriskmeetup.com

The future of data breaches, cyber resilience and incident response

By
Alan **Hartstein**
ACSM Correspondent

Sydney's latest Cyber Security Meetup not only drew a record crowd but was largely successful in demystifying the complex issues of data breach and incident response to an eclectic audience of lawyers, tech-heads and crypto and blockchain enthusiasts.

The three speakers all offered personal insights into the increasingly globalised world of data connectivity and how breaches affect everyone from multinationals to anyone with a MyHealth record or a Facebook account.

First up was Olga Ganopolsky, General Counsel, Privacy and Data, at Macquarie Group, who is responsible for all of the 28 jurisdictions Macquarie operates in. With her extensive knowledge of the data and privacy space, she was able to provide valuable insights into how lawyers view the issue in an international context and the current shape of data breach regulation globally.

"Data breaches take everyone out of their comfort zones, including lawyers," she says. "If data is global, the question then becomes how relevant are local laws?"

While some global frameworks have already taken shape, such as the European Union's General Data Protection Regulation which came into effect in February this year, there was still a spectacular lack of uniformity for reporting and policing data breaches, Ganopolsky says.

In the EU, for example, organisations are obliged to notify authorities within 72 hours of a data breach, while in the US the laws change from state to state and New York actually has three separate regulators responsible for data breach.

This lack of uniformity runs not only across nation states, but cultures and in some cases, such as the US, even across industries. This means that something which is deemed immediately notifiable in Australia may not be considered worthy of notification in a country such as The Philippines, which is rapidly becoming a hub for global outsourcing.

Then there's the added layers of complexity when it comes to ascertaining where the breach originated and who was responsible, made all the more complicated if, for example, a service provider inadvertently did something to a customer's IT platform or infrastructure.

Ganopolsky believes it is still possible to operate in such a regulatory minefield and, from a legal standpoint, understanding the regulatory framework of the country where the breach has occurred is essential, however difficult that may be. "Facts are important, but context is essential, and that involves making a real effort to understand the quirks of the country or territory in question."

Being human-centric and understanding the people who have been affected and how it has affected them is also vitally important in a globalised environment, she says, especially since the current gap in global frameworks is not going to be rectified anytime in the near future and cultural sensitivities will always be prevalent.

Keep your incident response simple

Dr Ignatius Swart, a security professional of more than 15 years standing, is a Managing Consultant of Privasec and also leads the NSW GRC and Incident Response teams. He was largely in accord with the previous speaker's comments on the complexity of the issue, especially in light of huge data breaches to the likes of Facebook, a plethora of banks and high-profile cases such as dating site Ashley Madison.

Having said that, he believes there are some simple steps organisations can take to greatly reduce the risks of such breaches. "First and foremost, there need to be defensive systems in place for when a breach occurs. Knowing where and why it happened will go a long way towards remedying it," Swart says.

Swart recommends a return to basics, where there is a simple security framework in place with a tested plan with clearly defined roles for those responsible across an organisation.

Often there are procedural steps that hinder incident response, like failure to withdraw password authorisation for users whose machines might be affected, especially if the attack occurs after hours when there's virtually nobody around.

Then there was the time when a major multinational suffered a major data breach which affected some very large customers, several of whom sent in their own incident response teams, with predictably disastrous consequences.

"This company ended up spending over 50 per cent more on fixing the breach than they should have because they didn't have proper response systems in place," Swart says.

Instead, they should have tested their environment for internal and external threats, given staff better training on what to do if an incident occurs, and above all else kept calm, he adds.

Regarding the future, Swart believes drones, AI and blockchain (all the major buzzwords, as he put it), will have a positive role to play in data security: drones through their high-speed computing platforms, AI through its potential to investigate breaches and remedy them and blockchain through its ability to provide an evidentiary link for every computing chain.

"Preparation is always better than response and communication between stakeholders is essential for post-incident reviews," Swart adds.

Data breaches affect everyone

Finally Andre Jenkins, the leader of CEC's Analytics Strategy, offered some unique insights into the risks everyone faces to their privacy and what can be done to keep their data secure.

He also provided the bulk of the mirth for the evening, with special reference to Facebook's Mark Zuckerberg spending untold millions to purchase surrounding houses in Palo Alto to ensure his privacy while being seemingly flippant about the data privacy of the hundreds of millions of ordinary folk who use his platform.

What made his talk especially interesting though was his posing the question of whether anyone could guarantee privacy now or going forward and whether it would still be as relevant in the future.

"If data is the new world order, we need to make informed decisions about a product that changes all the time," he says.

His example of health data was a powerful one, judging by the audience's response. It used to be that credit card fraud was the most feared form of data breach, but now you just report what happened and get most or all of your money back.

"Loss of health data, on the other hand, could lead to identity theft or the loss of your job if it fell into the wrong hands," he opined, "especially in the future when it may become much harder to differentiate between what's real and what's stolen."

This, he adds, is why Care.data, the UK equivalent of Australia's MyHealth, is now defunct after a relatively short period of time as people stopped trusting the government to be responsible custodians of their most intimate information, even allowing for the myriad of benefits that belonging to such a system brings with it.

The upshot of all of this, Jenkins adds, is that for someone with no technical knowledge, privacy and data breach concerns can be overwhelming, and that is likely to remain the case for the foreseeable future.

Privasec's Chief Offensive Officer, and leader of the Red Team Karan Khosla sharing real life case studies with the audience. Photo Credit: ICE71

A Cyber Risk meetup Exclusive & special speaker event with ICE71

By
Jane Lo
Singapore Correspondent

Breaking into a building, accessing the hidden world of a rogue intruder, and other "war stories" were shared at the third edition of the Cyber Risk Meetup held on 1st November, 2018 at JustCo in the heart of Singapore's Central Business District. Co-organized with ICE71, the region's first cybersecurity entrepreneur hub founded by Singtel Innov8 (corporate venture capital unit of Singtel), and NUS (National University of Singapore), the sell-out event of security practitioners and enthusiasts networked and shared best practices, thoughts and experiences on defending against the rapidly growing cybersecurity risks in the region.

Keynoting the event was lessons learned from Red Teaming exercises. As opposed to traditional assessments such as Penetration Testing, which may be scoped to focus only on technical risk. Red teaming assesses the organisation's business risk and its ability to detect and respond to incidents

Privasec's Chief Offensive Officer, and leader of the Red Team Karan Khosla, revealed two real-life case studies and the role social engineering played in gaining unauthorised access to buildings and secured areas.

Most non-practitioners may over-estimate the effort and time spent on the actual attack phase, but in fact, he said, "most of the cases, reconnaissance takes up the 90% of time".

Typical techniques to bypass physical access controls include looking legitimate (e.g. putting on officious looking uniforms), tailgating (following smokers back into the buildings via fire-exit doors), claiming false credentials in requesting for information such as access cards (and replicating them).

Another common technique is phishing, to extract confidential information such as user ID and passwords. In a case recounted by Karan, the password opened up access to a master mailbox that led to several inboxes of the senior executives.

The key to defend and protect against these social engineering attacks is identifying the weakest link – and usually this means enhancing security awareness of staff.

This was one of the key messages of the discussion panel.

Panelist Steve Ng (Lead, Digital Operations & Platforms, Mediacorp), David Robinson (CTO, STT Connect) and Viktor Pozgay (CISO,Avaloq Sourcing APAC), moderated by Shamane Tan (APAC Cyber Security Advisor) emphasised that whilst there are growing sophistication of attackers and number of breaches, there are basic Cyber Hygiene measures that can be adopted by everyone.

Exercising caution over the use of devices such as USBs, and adopting encryption when transmitting confidential and sensitive information are some well-known examples.

Panelist (Steve Ng (Lead, Digital Operations & Platforms, Mediacorp), David Robinson (CTO, STT Connect) and Viktor Pozgay (CISO,Avaloq Sourcing APAC), moderated by Shamane Tan (APAC Cyber Security Advisor). Photo Credit: ICE71

ICE71 organisers welcoming guests to the Cyber Risk Meetup 1st Nov 2018 event at JustCo, Singapore. Photo Credit: ICE71

Panelist (Steve Ng (Lead, Digital Operations & Platforms, Mediacorp), David Robinson (CTO, STT Connect) and Viktor Pozgay (CISO,Avaloq Sourcing APAC), moderated by Shamane Tan (APAC Cyber Security Advisor). Photo Credit: ICE71

Prashant Haldankar, CISO Privasec raising a question to the panel. Photo Credit: ICE71

Interestingly, while brute-forcing password may be a way to access a google email or Hotmail account, most hackers seek to reset passwords relying on answers found on social media to "what is your pet's name". The lesson is that whilst secure passwords are critical, minimal divulging of personal information on social media or other public platforms is also crucial.

Key best practices for enterprises were also highlighted during the 30-minute panel discussion. (LIVE FEED LINK HERE)

Gaining senior management level buy-in into cyber security polices and strategies is a priority, according to Viktor Pozgay (CISO,Avaloq Sourcing APAC).

Rapid remediation is an important defence when there is an incident. "When you have an intruder in your network, the question you need to ask yourself is how fast can you remediate", and "if you find that it takes you weeks to patch, start making changes now", said David Robinson (CTO, STT Connect).

Engaging a variety of vendors for different parts of security is also part of effective security risk management, to minimize single point of failure whether through legitimate or illegitimate methods, according to Steve Ng (Lead, Digital Operations & Platforms).

"People is your most important asset", Steve said. Incidents need to be identified as early as possible, and with staff who are knowledgeable with the right skills and experience, they would be able to identify early warning signs and any anomalous behavioural patterns. "No one does the attack on day 1, there are leading indicators", David agreed.

So, whilst the weakest link may be the staff, they are also key to protecting the organisation against attacks.

"Educate your people", said Steve. Indeed, raising awareness of the cyber security landscape and the part that everyone can play in protecting the organisation is the ultimate best defence.

Register at **promoteme@mysecuritymedia.com**
or visit **www.cyberriskmeetup.com**

See you next time!

Feel free to drop us a line to refer us speakers and partners...

CYBER RISKERS

Proudly supported by

MYSECURITY MEDIA APP

MYSECURITY MARKETPLACE

CYBER RISK LEADERS

AUSTRALIAN CYBERSECURITY MAGAZINE

Cyber Security WEEKLY PODCAST