

CISO Brisbane

▶ Connecting you to what's next in InfoSec

| CISO BRISBANE 24 th June 2025 | |
|---|--|
| 08:00 | <i>Register; grab a coffee. Mix, mingle and say hello to peers old and new.</i> |
| 08:45 | <p>Welcoming Remarks by Corinium and Chair's Opening Remarks</p> <p><u>Chair:</u> Sanja Marais CTSO Aspen Medical</p> <p><u>Corinium Representative:</u> Kashmira George Content Director Corinium Global Intelligence</p> |
| 08:50 | <p>Speed Networking – Making new connections at CISO Brisbane!</p> <p>During this 10-minute networking session, the aim of the game is to go and meet three people you don't already know. Use the questions on the screen to guide your conversation. Have fun!</p> |
| 9:00 | <p>The Journey of a CISO: From IT to Influencer</p> <ul style="list-style-type: none"> • Evolving the CISO Role from a technical expert to a strategic leader by balancing accountability • Navigating board expectations, budget constraints and regulatory pressures • Fostering sustainable leadership in high-stakes environments <p>Fabian Llanos Lopez Principal Advisor, Information Management and Security Department of Natural Resources and Mines, Manufacturing and Regional Rural Development</p> |
| 09:25 | <p>Ransomware Unmasked: How to Prevent, Detect, and Respond to Modern Threats</p> <ul style="list-style-type: none"> • Introduction – What is ransomware? Why is it a growing threat? • Attack Lifecycle – How ransomware infiltrates, spreads, and executes. • Real-World Case Studies – Lessons from high-profile ransomware attacks. • Prevention & Defence Strategies – Zero Trust, threat intelligence, and security best practices. • Incident Response & Recovery – What to do if you're hit and how to recover quickly. <p>Matt O'Kane Director Notion Digital Forensics, Distinguished Lecturer UNSW & Cloudflare Advocate Cloudflare</p> |
| 09:50 | <p>Case Study</p> <p>Regulatory Burdens or Business Enablers: Balancing Compliance and Risk to Deliver Meaningful Security Uplift while Enabling Innovation and Growth</p> <ul style="list-style-type: none"> • Viewing cyber security as not just as a protective measure but as an enabler for business innovation and trust |

| | |
|-------|---|
| | <ul style="list-style-type: none"> Aligning business strategy with key security outcomes and targets to strengthen overall organizational maturity Delivering prudent, risk-based security outcomes to enable business change while achieving compliance targets <p>Jon Coleman GM, Cyber and Information Security Energy Queensland</p> |
| 10:15 | <i>Coffee and Connect</i> |
| 10:45 | <p>Panel Discussion</p> <p>The Human Element: Strengthening Cyber-Awareness Beyond the Enterprise</p> <ul style="list-style-type: none"> Fostering a 'security-first' culture and leveraging tools to reduce human error effectively Highlighting the importance of collaborative efforts and community initiatives to enhance awareness of phishing and newer threats Transforming the 'weakest link' narrative into a culture of accountability and vigilance <p>Moderator Guillaume Noé Head of Cyber Resilience Queensland Government</p> <p>Panellists: Glen Gooding Head of Information Security WorkCover Queensland Nikki Peever Director Cyber Security CAUDIT Rob Wiggan Senior Cyber Security Advisor</p> |
| 11:20 | <p>From Vulnerability to Vanguard: Reinventing DNS Security</p> <p>In today's digital world, security challenges are evolving rapidly. As Australia aims for ambitious security goals, the need for cost-effective solutions is rising. Domain Name System (DNS) technology holds immense potential yet many organisations don't fully understand its role in security. We will highlight DNS vulnerabilities, threats exploiting the protocol and security approaches using DNS to defend against cyber threats. Learn about DNS's importance, vulnerabilities and how to leverage it for defence, gaining insights into threat detection and mitigation to bolster your security posture.</p> <p>Brad Ford Security Specialist – ANZ Infoblox</p> |
| 11:45 | <p>Interactive Incident Drill: The CEO's Calendar Glitch</p> <p>In this facilitated session, teams will be presented with a cyber incident scenario and tasked with forming a response under time constraints. Explore how different leadership styles, instincts, and strategies play out when the heat is on.</p> <p>What would you do if your CEO's calendar vanishes and your SOC flags suspicious login activity? In this 25-minute challenge, each table becomes a mini-incident response team. Collaborate, investigate, and present your final theory.</p> <p>What would you escalate, who would you call, and what lessons would you walk away with?</p> <p>Facilitator Sanja Marais CTSO Aspen Medical</p> |
| 12:10 | <p><i>Lunch</i></p> <p>Private Luncheon hosted by Delinea (Invite Only)</p> |

This document is a draft agenda and subject to change. It is confidential and only intended for the designated recipient. Please do not copy, reproduce, or distribute this document without the consent of the sender.

©Corinium Global Intelligence

| 13:10 | Track A: Resilience and Maturity Chaired by Sanja Marais CTSO Aspen Medical | Track B: Tech, Threats and Transformation Chaired by Dan Haagman CEO Chaleit |
|-------|---|---|
| | <p>Creating a Risk Resilient Culture by Making Cyber security a Boardroom Priority</p> <ul style="list-style-type: none"> Transforming legislative compliance into proactive organizational culture Bridging gaps in maturity with practical steps for CISOs to align with boards Preparing for upcoming changes in privacy laws, from stricter enforcement to aligning with global frameworks like GDPR <p>Glenn Dickman Director Cyber Security Griffith University</p> | <p>Case Study Beyond the Weakest Link: A Roadmap to Cyber Awareness & Engagement</p> <ul style="list-style-type: none"> Reframing cyber security awareness to make employees active participants, not liabilities. Creating cost-effective campaigns and maximizing the impact of cyber-awareness Tactics for shifting mindsets and engaging an indifferent workforce while maintaining compliance. Moving beyond the “weakest link” narrative to drive a culture of shared cyber responsibility. <p>Felipe Abreu Head of IT Infrastructure & Cyber Security VAE Group</p> |
| 13:35 | <p>Rethinking Detection in a Decentralised World</p> <p>In the modern enterprise responding to cyber threats is harder than ever. Even the largest businesses with vast resources are getting breached.</p> <p>In this session we'll discuss a new approach to detect and respond faster, to help keep enterprises running even when a breach occurs, and how we can stay one step ahead of the most advanced threat actors.</p> <p>Lee Evans Regional Sales Director Illumio</p> | <p>Navigating Digital Transformation Safely</p> <p>Digital innovation isn't optional—it's the engine of modern business growth, driving sharper customer experiences, operational efficiency, and bottom-line impact. But this momentum comes with risk.</p> <p>As organisations accelerate transformation, cybersecurity must evolve just as fast. In this session, we unpack how security leaders can move from blockers to enablers—managing emerging risks, embedding structured resilience, and using AI to fuel secure innovation at scale.</p> <ul style="list-style-type: none"> Managing Cyber Risks in Digital Transformation – Identify and mitigate the fast-evolving threats that come with rapid innovation and tech adoption. Proactive Risk Assessment – Use structured, risk-based methods to boost resilience, maximise return on security investments, and ensure compliance. AI for Cyber Defence & Innovation – Harness AI not just to defend, but to accelerate secure innovation—automating response, reducing risk, and enabling scale. |

This document is a draft agenda and subject to change. It is confidential and only intended for the designated recipient. Please do not copy, reproduce, or distribute this document without the consent of the sender.

| | | |
|-------|--|---|
| | | Andrew Philp Field CISO, ANZ Trend Micro |
| 14:00 | <p>Case Study Building a Risk Based Cyber Security Strategy: An AI Adoption Roadmap</p> <ul style="list-style-type: none"> • Developing an organisational AI roadmap that enhances cyber security resilience and business alignment. • Leveraging AI for efficiency while maintaining ethical decision-making and control. • Implementing AI in cyber security while ensuring transparency, fairness, and regulatory adherence. • Showcasing how organisations are leveraging AI to transform their security strategies. <p>Dane Warren Head of Information Security IOR Group</p> | <p>Panel Discussion Innovation Meets Compliance: Aligning Cyber Defences with Upcoming Regulatory Developments</p> <ul style="list-style-type: none"> • CPS 230: Addressing APRA's new operational risk standard for enhanced governance and incident management in critical sectors. • Mitigating reputational risks from weak enforcement and exploring practical strategies to integrate these frameworks for operational efficiency • Complying with CPS 234, CPG 234, CPG 235, and other standards such as ISO27001, NIST and Essential 8 <p>Moderator Ryan Ko Director of Research/Founding Director of UQ Cyber Research Centre The University of Queensland</p> <p>Panellists Jeremy Leong Chief Risk Officer, Head of Risk and Compliance Taishin International Bank – Brisbane Branch Ejaz Ahmed Cyber Security Operations Lead Airservices Australia Richard Carter Head of Cyber and Information Security Brighter Super</p> |
| 14:25 | <p>How DevSecOps Platforms Help Secure the Software Supply Chain</p> <p>As organizations accelerate digital transformation initiatives, they face mounting pressure to harmonize rapid software delivery with robust security measures. This session explores how the convergence of DevSecOps, Artificial Intelligence, and Value Stream Management (VSM) creates a comprehensive framework for secure, efficient software development.</p> <p>We'll examine practical strategies for integrating AI-powered security controls into development pipelines, leveraging VSM metrics to optimize security processes, and building resilient software supply chains.</p> | <p>Less Spend, More Security: Optimizing Tools & Reducing Costs in 2025</p> <ul style="list-style-type: none"> • Optimize Security, Cut Costs – Improve security while reducing spend. • Modernize Data Infrastructure – Shift from static to flexible, composable architectures. • Future-Proof IT & Security – Adapt strategies to stay resilient for the next decade. <p>Jenna Eagle Director Solutions Engineering Cribl</p> |

This document is a draft agenda and subject to change. It is confidential and only intended for the designated recipient. Please do not copy, reproduce, or distribute this document without the consent of the sender.

©Corinium Global Intelligence

| | | |
|-------|---|---|
| | <p>Join us to unlock a seamless delivery pipeline, fortified security, and enhanced business value amidst the ever-evolving threat landscape.</p> <p>Robert Williams Senior Solutions Architect GitLab</p> | |
| 14:50 | <p>Panel Discussion AI in Cyber Security: Enabler, Risk or Distraction?</p> <ul style="list-style-type: none"> Understanding AI's dual role: as a tool for defense and an enabler of sophisticated attacks. Examining real-world examples of AI-driven phishing, deepfakes, and targeted cyber campaigns How Australian organizations can use AI responsibly to strengthen their cyber security programs. <p>Moderator Gaurav Vikash Head of Security and Risk AXON</p> <p>Panellists Michael Poezyn Chief Security Officer Derivco Andy Vadlamani Head of Information Security Compare the Market Adam Plotnikov Senior Solutions Engineer BigID</p> | <p>Fireside Chat Securing Cloud Continuity: Overcoming Challenges with Legacy Systems</p> <p>As the industry evolves, maintaining continuity while managing legacy systems is crucial. This session will explore how can ensure business continuity by implementing robust backup strategies and addressing the risks of outdated systems. We'll discuss how legacy systems may fall short of modern cyber security standards and share insights on upgrading into cloud infrastructure to safeguard client data and ensure seamless operations.</p> <p>Moderator Dan Haagman CEO Chaleit</p> <p>Panellists John Heaton Head of Strategy and Innovation Alex Bank Marc Reinhardt Director, Cyber Security and IT Risk ICON Group James Court Chief Security Officer Cleanaway Waste Management</p> |
| 15:15 | <p>Keynote Beyond the Phishing Test: Effective Strategies for Managing Human Risk</p> <p>68% of all data breaches are due to human error, and despite significant investments in technical safeguards, phishing and social engineering attacks remain the #1 threat to your organisation.</p> <p>This session will explore:</p> <ul style="list-style-type: none"> The critical shift from traditional security awareness to human risk management (HRM). How social engineering and phishing—particularly via email—remain the primary vectors for breaches and ransomware, now amplified by AI technologies that make sophisticated attacks accessible to novice cybercriminals. | <p>Keynote Securing Data in the Age of AI: Risks, Innovations, and Best Practices</p> <p>During this session, we will show you just how easily your company's sensitive data can be exposed using Microsoft Copilot with simple prompts. We will share practical steps and strategies to ensure a secure Microsoft Copilot rollout and prevent prompt hacking data exposure.</p> <p>Geoff Morrison Manager of Sales Engineering, ANZ Varonis</p> |

This document is a draft agenda and subject to change. It is confidential and only intended for the designated recipient. Please do not copy, reproduce, or distribute this document without the consent of the sender.

©Corinium Global Intelligence

| | | |
|-------|---|--|
| | <ul style="list-style-type: none"> Explore frameworks to quantify human risk, establish meaningful benchmarks and provide clear metrics to measure success. <p>Joe Gillett Head of ANZ KnowBe4</p> | |
| 15:40 | <i>Coffee and Connect!</i> | |
| 16:10 | <p>Cyber in 5: Key Insights from Cythera's CISO Survey A quick, 5-minute dive into how Cythera leverages security automation to dramatically reduce response times and eliminate noise, enabling our security operations team to focus on what truly matters—real threats and meaningful customer engagement.</p> <p>Tim Sank Co-Founder Cythera</p> | |
| 16:15 | <p>Panel Discussion Creating a Resilient Mindset in Cyber Security Teams</p> <ul style="list-style-type: none"> Fostering mental resilience in cyber teams, balancing workload and maintaining focus during high stakes crises. Aligning CISO goals with board level business objectives to enhance longevity and maturity Highlighting the importance of mentorship, peer support and resources for CISOs The role of CISOs in shaping policies, standards, and global cyber security initiatives for mental health <p>Moderator Sanja Marais CTSO Aspen Medical</p> <p>Panellists Stephen Bennett CISO Domino's Amanda Pinaud Cyber Security Manager MegaPort Gabriela Guiu-Sorsa Community Founder and Mentor Cyber Security Champions of Tomorrow</p> | |
| 16:50 | <p>Case Study Securing Brisbane's Supply Chain from Small Business Vulnerabilities to Large Enterprise Risks</p> <ul style="list-style-type: none"> Best practices for vetting and securing third, fourth, and fifth parties, ensuring that all links are protected Strengthening collaboration and establishing comprehensive cyber security standards that cover all levels of the supply chain, from small businesses to large enterprises Strengthening supply chain security by ensuring continuity, and mitigating risks that stem from interconnected business relationships <p>Hitesh Jamb DevSecOps and Test Practice Lead APA Group</p> | |
| 17:15 | Chair Closing Remarks | |
| 17:25 | <p>Cheers with Peers <i>Join us for a time of networking and drinks!</i></p> | |
| | Close of CISO Brisbane 2025 | |

This document is a draft agenda and subject to change. It is confidential and only intended for the designated recipient. Please do not copy, reproduce, or distribute this document without the consent of the sender.

©Corinium Global Intelligence