7 CYBERSECURITY, DATA BREACH & DATA PRIVACY FORUM

12 November 2025
PierOne Sydney Harbour

Gold Partner

airia
Secure Legal AI

Supporting Association

AUSCL

Produced by :

ChilliIQ
connecting leaders + ideas

Thomson Reuters™

about ChilliIQ

connecting leaders + ideas

We are a leading creator of conferences and summits who aim to bring together great minds with avid learners amongst the thought-inspiring atmosphere of leading venues.

Chilli IQ has many years of collective experience in the area of creating and developing innovative conferences and summits for the changing business environment. This is not though what differentiates us from the crowd, what makes us unique is our modus operandi.

We value quality and strive to ensure that every aspect of our events reflects this – from the choice of speakers, the venue and the genuine attention to detail.

Our main objective is to lead the field in the area of knowledge delivery and as this is a fluid process we are constantly seeking new avenues and evolving to make sure we never just settle.

We ensure that all who partake in the Chilli IQ conference experience – whether it be as a delegate, a speaker, a sponsor or an endorsing association – maximise their investment and attain a higher level of understanding and awareness of the chosen business theme.

ChilliIQ conferences are always relevant and presentations provide content that you didn't even know you wanted to know! Great way to network with old contacts and forge new ones.

[past delegate]

about the **event**

Securing the Digital Future: evolving threats – smarter responses

As digital transformation accelerates, the threats to data security and privacy grow more complex. The Cybersecurity, Data Breach & Data Privacy Conference 2025 will bring together leading experts to explore the evolving landscape of cyber threats, regulatory frameworks, and innovative solutions.

There has been an unprecedented wave of cyber threats, with data breaches affecting millions and disrupting key sectors such as finance,legal, healthcare, and government. High-profile incidents—including those involving Medibank and Optus—have exposed critical vulnerabilities and eroded public trust. As cybercriminals rapidly evolve their tactics, employing methods like credential stuffing, deepfakes, and AI-driven attacks, Australia must respond with a united front—through innovation, strengthened regulation, and cross-sector collaboration.

The upcoming 7th Cybersecurity, Data Breach, and Data Privacy Forum aims to tackle these crucial issues that impact businesses. The agenda is meticulously designed to highlight the latest cybersecurity technologies and tactics, providing valuable insights into how companies can address these ever-evolving threats.

“Cybersecurity is not just a technical challenge, but a strategic imperative for business survival in a world increasingly reliant on digital infrastructure."

what you will **learn**

The event will cover the following crucial topics:

- **THE EVOLVING CYBER THREAT LANDSCAPE**
- **DATA BREACHES AND INCIDENT RESPONSE: LESSONS FROM MAJOR CYBER CASES : MEDIBANK, OPTUS AND OTHERS**
- **NAVIGATING AUSTRALIA'S PRIVACY REGULATIONS AND GLOBAL COMPLIANCE : OAIC GUIDELINES, PRIVACY ACT REFORMS & GDPR**
- **CYBERSECURITY BY DESIGN: BUILDING RESILIENT SYSTEMS AND INFRASTRUCTURE**
- **THE HUMAN FACTOR: SOCIAL ENGINEERING, PHISHING, AND INSIDER THREATS**
- **THE ROLE OF CYBER INSURANCE POST-BREACH, POLICY EXCLUSIONS, AND HOW INSURERS ARE RESPONDING TO GROWING THREATS.**
- **THE FUTURE OF CYBERSECURITY**
- **THE DOUBLE-EDGED SWORD OF AI IN CYBERSECURITY: EXPLORING THE OPPORTUNITIES AND CHALLENGES**

who should **attend**

This event has been exclusively produced to address the function and capacity of the following position:

• CSOs, CISOs, CROs, CPOs and their teams
– Security and risk management
– Business/IT security alignment
– IT/OT security integration
– Governance and policy setting
– Creating a risk-aware culture
– People-centric security

• Security leaders
– Network security leaders
– Mobile application and security
– Social media & security
– Advanced targeted threats
– Incident response
– Cybersecurity
– Cloud computing security

• Governance, risk and compliance consultants
– Digital risks in financial services
– Operational technology risks
– GRC application strategy
– Information governance
– Big data litigation and regulatory risks

• Business continuity and IT disaster recovery managers
– BCM program management
– BCM standards and organisation
– Supplier management/third party risk

• Security Architects

• Network and Systems Security Administrators

confirmed **speakers**

The following speakers have been invited for their expertise and knowledge on the chosen topics:

- **BRENTON STEENKAMP** PARTNER | HEAD OF CYBER & DATA GOVERNANCE **CLAYTON UTZ**
- **DR GEORG THOMAS** DIRECTOR **DRGT CONSULTING**
- **DR ALLISON STANFIELD** PARTNER **LEWIS DENLEY**
- **DR. QIANG TANG |** ASSOCIATE PROFESSOR - COMPUTER SCIENCE **THE UNIVERSITY OF SYDNEY**
- **KATHERINE JONES** PARTNER **COLIN BIGGERS & PAISLEY**
- **MAGDALENA BLANCH-DE WILT** APAC CYBER RISK ADVISORY LEAD + EXECUTIVE COUNSEL **HERBERT SMITH FREEHILLS KRAMER**
- **LEAH MOONEY** TECHNOLOGY, CYBER AND PRIVACY CONSULTING LEADER, PACIFIC **WILLIS, A WTW BUSINESS**

CLICK HERE TO REGISTER ONLINE

ChilliIQ

Programme

8:30 - 9:00
Registration

Registration Open

9:00 - 9:15
Start of Forum

Introduction from the Chair & Start of Forum

SESSION 1
9:15 - 10:00

THE EVOLVING CYBER THREAT LANDSCAPE

The cyber threat landscape is undergoing rapid transformation, posing significant legal and regulatory implications for organisations and their advisors. Traditional risks—such as malware and phishing—remain prevalent, but are increasingly overshadowed by complex threats including ransomware attacks, supply chain compromises, and the exploitation of emerging technologies such as artificial intelligence, cloud computing, and the Internet of Things.

These developments have expanded the scope of potential liability for organisations. Cyber incidents frequently engage privacy, contractual, and regulatory obligations, and may trigger mandatory reporting requirements under privacy and critical infrastructure legislation. They also raise issues concerning directors' duties, professional negligence, and the adequacy of contractual risk allocation in digital services and supply chains.

At the same time, regulators are adopting a more proactive stance on cybersecurity governance and disclosure obligations, particularly in the financial services and corporate sectors. Legal practitioners must therefore remain attuned to evolving threat vectors, not only to advise on compliance and risk management, but also to anticipate litigation, regulatory enforcement, and reputational consequences arising from cyber incidents.

DR ALLISON STANFIELD PARTNER **LEWIS DENLEY**

SESSION 2
10:00 - 10:45

TOWARDS END-TO-END ENCRYPTED ONLINE COLLABORATIONS

Despite the pervasiveness of cloud platforms that facilitate outsourced storage and online collaborations, the basic requirement of end-to-end security is not yet available. As a consequence, we've witnessed many massive scales data breaches, frequently. This is in sharp contrast with communication, that there are long sequences of research and practical systems for end-to-end encrypted messaging available.

In this talk, I will overview the key challenges causing this mismatch, and our recent efforts of providing end-to-end security for cloud storage and Git services with rigorous guarantees, while preserving full compatibility with existing infrastructure, and incurring only minimal overhead.

DR. QIANG TANG | ASSOCIATE PROFESSOR - COMPUTER SCIENCE
THE UNIVERSITY OF SYDNEY

10:45 - 11:15
Break

Morning Break and Time to Chat

Programme

TECH TALK
11:15 - 11:30

AI GOVERNANCE IN LEGAL PRACTICE: FROM RISK TO STRATEGIC ADVANTAGE
Attorneys and staff are adopting AI tools at a rapid pace—often without IT oversight or governance. While this enthusiasm for innovation is promising, it creates serious risks: breaches of client confidentiality, ethical violations, and even malpractice exposure.

Join us to learn how leading law firms and corporate legal teams can address shadow AI as both a risk and an opportunity—protecting client privilege while gaining a competitive edge.

RICHARD DAVIES REGIONAL SALES LEAD ANZ **AIRIA**

SESSION 3
11:30 -12:15

NAVIGATING AUSTRALIA'S PRIVACY REGULATIONS: WHERE WE CAME FROM AND WHERE WE ARE GOING?
In this session Katherine will explore the events leading up to the Privacy Act 1988, and how the world has changed bringing us to the latest round of changes to the Privacy Act including the new tort of privacy and civil penalty provisions.
KATHERINE JONES PARTNER **COLIN BIGGERS & PAISLEY**
Katherine Jones leads the breach response team at Colin Biggers & Paisley. With 17 years of litigation experience across Australia and Hong Kong, she began her cyber law career in Hong Kong eight years ago before returning to Australia to build Colin Biggers & Paisley's cyber practice. Katherine supports clients through cyber incidents, offering clear advice and decisive action when it matters most. Her work also spans fraud defence, white collar crime, and regulatory investigations. She was a finalist for Cyber Security Lawyer of the Year at the 2025 Australian Cyber Awards.

12:15 - 13:15
BREAK

Lunch Break and Time to Chat

SESSION 4
13:15 - 14:00

THE HUMAN FACTOR: SOCIAL ENGINEERING, PHISHING, AND INSIDER THREATS
This session will explore the critical role of humans in cyber security, focusing on social engineering, phishing and insider threats. The "human factor" can undermine even the most advanced technical defences. The rise of artificial intelligence by threat actors has elevated the level of sophistication when conducting attacks and organisation's need to be prepared. The session will conclude with a look at human-centric defence measures and how to foster a culture of security.
DR GEORG THOMAS DIRECTOR **DRGT CONSULTING**

Programme

SESSION 5
14:00 - 14:45

CYBERSECURITY BY DESIGN: BUILDING RESILIENT SYSTEMS AND INFRASTRUCTURE

BRENTON STEENKAMP PARTNER | HEAD OF CYBER & DATA GOVERNANCE
CLAYTON UTZ

14:45 -15:15
BREAK

Afternoon Tea and Time to Chat

SESSION 6
15:15- 16:00

THE DOUBLE-EDGED SWORD OF AI IN CYBERSECURITY: EXPLORING THE OPPORTUNITIES AND CHALLENGES

There's concern amongst directors and executive leadership teams that the surge in AI technologies has brought a step change to the cyber security risk landscape. Threat actors are increasingly weaponising artificial intelligence (AI) to enhance the scale, speed, and sophistication of cyberattacks. At the same time, organisations are implementing a range of strategies to respond to AI-driven cyber threats, including through the use of AI based tools.

Join Magda to take a closer look at the status of the arms race, how organisations are responding, what teams advising clients on cyber incidents are seeing "on the ground", and what it means for our organisations for 2026 and beyond from a governance, risk, legal and compliance perspective.

MAGDALENA BLANCH-DE WILT APAC CYBER RISK ADVISORY LEAD + EXECUTIVE COUNSEL **HERBERT SMITH FREEHILLS KRAMER**

SESSION 7
16:00 - 16:45

THE FUTURE OF CYBERSECURITY
LEAH MOONEY TECHNOLOGY, CYBER AND PRIVACY CONSULTING LEADER, PACIFIC **WILLIS, A WTW BUSINESS**

16:45 -17:00
CLOSING REMARKS

CLOSING REMARKS FROM THE CHAIR

17:00 - 18:00
DRINKS AND END OF FORUM

POST - EVENT DRINKS AND END OF FORUM

event information

EVENT NAME: **7th CYBERSECURITY, DATA BREACH & DATA PRIVACY FORUM**

EVENT DATE: **12 NOVEMBER 2025**

VENUE: **PIER ONE SYDNEY HARBOUR**
11 Hickson Road, Walsh Bay, Sydney NSW 2000 Australia

CONFERENCE TIMING:

CONFERENCE REGISTRATION:	8.30AM- 9.00AM
CONFERENCE TIMING:	9.00AM- 5:00PM
NETWORKING DRINKS:	5:00PM - 6:00PM
DRESS REQUIREMENTS:	SMART CASUAL

DELEGATE RATE

DELEGATE RATE : **$495.00***

SPECIAL GROUP RATE *PER DELEGATE **$395.00***

include code **CIQCYBER25** when registering under payment details **promotional code**

*** This rate is extended to WHO SHOULD ATTEND only please see page 4**

- 1-Day Conference Pass
- Conference luncheon & refreshments including post event drinks
- Delegate bag
- Exhibition Pass
- Conference Slides that have been approved for publication will be emailed after the event

*ALL **AUSCL** MEMBERS GET ANOTHER **10% DISCOUNT OFF**

include code **AUSCL10** when registering under payment details **promotional code AUSCL10**

SERVICE PROVIDER / CONSULTANTS REGISTRATION* **$1,295.00**

email george.kat@chilliiq.com.au to secure this rate

event information

EVENT NAME:	**7th CYBERSECURITY, DATA BREACH & DATA PRIVACY FORUM**
EVENT DATE:	12 NOVEMBER 2025
VENUE:	**PIER ONE SYDNEY HARBOUR** 11 Hickson Road, Walsh Bay, Sydney NSW 2000 Australia

CONFERENCE TIMING:

CONFERENCE REGISTRATION:	8.30AM- 9.00AM
CONFERENCE TIMING:	9.00AM- 5:00PM
NETWORKING DRINKS:	5:00PM - 6:00PM
DRESS REQUIREMENTS:	SMART CASUAL