CYBERSECURITY & BREACH RESPONSE BOOTCAMP

With more speakers to be announced!!

2026 Speakers

Dr Sharif Abuadbba (Sydney only)

Team Leader of Distributed Systems Security | AI & Cybersecurity, CSIRO's Data 61

Dr Sharif has over 14 years of experience leading national and international cybersecurity projects, including award-winning initiatives such as SmartShield, TAPE, and ThreatModelling-GPT. He has published 70+ papers in top security venues and serves as an Associate Editor for IEEE TIFS. Sharif is a CSIRO Julius Career Award recipient, recognised for advancing AI security, cyber defence, and protection against emerging threats like deepfakes and AI-driven attacks.

Clyde Netto

Regional Head of Technology and Cyber Security, Asia and Emerging Markets, Thomson Reuters

With 24 years of experience in the field, Clyde has held diverse roles in Software Development, Engineering, Cyber Security, Governance, Compliance, and Strategic Leadership. A Certified Information Systems Security Professional (CISSP) and a Certified Cyber Security Professional recognized by the Australian Computer Society, Clyde is dedicated to developing and securing intelligent systems that enhance and streamline complex legal and tax workflows, driving efficiency in these sectors.

Sam Fariborz (Brisbane, Melbourne only)

Chief Information Security Officer, David Jones

Sam is the CISO at David Jones, bringing technical expertise and leadership to cybersecurity, strategic leader skilled in translating cyber risk into business language for boards and executives while building high-performing, diverse security teams. She views security as an enabler of resilience and innovation, and has led transformation initiatives, embedding security into major digital programs. Sam is recognized as an industry leader and speaker, honoured as Australian Information Security Association (AISA)'s Cybersecurity 2024 Professional of the Year, and helps AISA in their mission as an executive committee board member.

Matthew Abbott

Corporate Affairs Leader, Ex-Latitude Financial, Zip, and ASIC.

Matthew Abbott is a Corporate Affairs leader with experience across financial services, fintechs, regulation and property, leading communications, government relations, and public policy functions in these sectors. Matthew has held senior Corporate Affairs roles in the listed world at Latitude Financial, Zip Co and Westfield, and spent nearly a decade leading corporate affairs at the Australian corporate watchdog ASIC. He was also an advisor to former treasurer Hon Joe Hockey and started his career as a reporter with the Australian Financial Review.
A seasoned strategist known for navigating complex regulatory and public environments, Matthew brings deep expertise in stakeholder engagement, media relations, and crisis communications—skills honed over two decades shaping communications for high-impact organisations.

Simone Herbert-Lowe

Partner, Clyde & Co

Simone is a partner in Clyde & Co's insurance practice and leads its Australian Cyber team. A recognised expert in cyber risk, privacy and legal liability, she advises on cyber incidents, insurance coverage, professional liability and cyber resilience. With over 30 years' experience across litigation, regulatory response and strategic risk advisory, Simone brings deep insight and practical leadership to this area. Combining sought after expertise in facilitating incident response exercises with the delivery of industry-leading cyber education, Simone's leadership has been recognised through awards for innovation, cybersecurity and ethical business practice.

2026 Programme - Sydney

08:00	Registration and arrival
08:30	**Welcome from MC** Clyde Nett, Thomson Reuters

Strategic Foundations

08:40	**Opening Keynote: Leading Cyber Risk in 2026** Dr Sharif Abuadbba (CSIRO)
09:25	**Privacy Law Update: Navigating Compliance** Simone Herbert-Lowe (Clyde & Co)
10:20	Moring Tea & Networking

Crisis Preparation

10:50	**Crisis Communications & Stakeholder Masterclass** Matthew Abbott (Ex-Latitude Financial, Zip Co, and ASIC)

Live Simulation

11:45	**Cyber Breach Response Workshop** Legal Lead: Simone Herbert Lowe Blue Team: Sam Fariborz, David Jones (Brisbane) Red Team: Clyde Netto, Thomson Reuters **Sydney Blue lead to be announced soon*

(includes 2x 10min breaks)

13:25	Lunch & Networking

Deep Analysis

14:15	**Simulation Debrief, Lessons Learned & Reflection** Expert perspectives from all facilitators on what worked, what didn't, and why
15:10	Afternoon Tea & Networking

Action Planning

15:40	**30-Day Action Plan + Board Reporting Workshop**
17:00	Event Close

Please note agenda is subject to change

CYBERSECURITY & BREACH RESPONSE BOOTCAMP

What's included in your registration fee

On the day

- Full-day bootcamp access with all sessions and workshops
- Live breach response simulation with expert facilitators
- Morning tea, lunch, and afternoon tea
- Networking opportunities with peers and industry experts
- Up to 7 CPD/CPE points

Resource Kit (provided on the day)

- 30-day action plan template
- Board presentation template
- Gap assessment framework
- Business case frameworks
- Simulation scenario details and role assignments

Post-Event Support (delivered within 1 week)

Complete Template Library:

- Incident response plan templates
- Crisis communication scripts
- Stakeholder communication calendars
- Decision trees and RACI matrices
- Board briefing templates
- Legal and regulatory checklists

Additional Resources:

- Invitation to 2027 masterclass with alumni discount
- CPD certificate of attendance - upon request

SESSION

Opening Keynote: Leading Cyber Risk in 2026

Get clear on what truly matters in the 2026 cyber risk landscape. With more than 14 years leading major cybersecurity initiatives, Dr Sharif breaks down emerging AI-driven threats such as deepfakes, automated attack campaigns, and machine-learning powered exploitation, and turns them into strategic priorities for boards and executive leadership.

He explains why 2026 marks a turning point, why traditional playbooks are no longer effective, and what organisations must prioritise now. This keynote connects technical realities with business decision-making and equips CISOs with the language and frameworks needed to elevate cyber risk conversations. It sets the strategic foundation for the bootcamp.

Key takeaways

- How AI-enabled attacks compress response windows and reshape threat intelligence
- Governance priorities for boards and CISOs including oversight models, risk appetite, and investment justification
- Global regulatory pressures such as EU NIS2, US SEC rules, and UK NCSC guidance influencing Australian expectations
- Insights from OAIC and SOCI Act enforcement and what 2025 signals for 2026 obligations
- Lessons from major 2025 breaches and what separated effective responses from failures
- The core cyber resilience investments that matter most in 2026
- How to translate technical risk into clear business language for board alignment
- Practical actions leaders can take this quarter to strengthen resilience

Speaker

Dr Sharif Abuadbba (Sydney only)
Team Leader of Distributed Systems Security | AI & Cybersecurity, CSIRO's Data 61

Dr Sharif has over 14 years of experience leading national and international cybersecurity projects, including award-winning initiatives such as SmartShield, TAPE, and ThreatModelling-GPT. He has published 70+ papers in top security venues and serves as an Associate Editor for IEEE TIFS. Sharif is a CSIRO Julius Career Award recipient, recognised for advancing AI security, cyber defence, and protection against emerging threats like deepfakes and AI-driven attacks.

SESSION

Privacy Law Update: Navigating Compliance

Privacy regulation is accelerating, and 2026 introduces tighter notification timelines, higher penalties, and far stronger expectations from regulators. In this session, Simone Herbert-Lowe, partner and head of Clyde & Co's Australian Cyber practice, provides a clear and practical breakdown of the changes that matter most for breach response. With more than 30 years advising on complex cyber incidents, regulatory investigations, and high-stakes compliance questions, Simone brings deep insight into how OAIC interprets obligations, what they view as acceptable practice, and where organisations are most exposed.

This session moves beyond a legal overview and focuses on real operational application. You will learn how to navigate OAIC notification rules under pressure, how to structure investigations to preserve legal privilege, and how to avoid the common compliance errors that create unnecessary penalties and prolong incident response.

Simone also highlights lessons from 2025 enforcement activity, showing how regulators are using new powers and what organisations must do differently in 2026 to meet expectations.

Practical templates, case examples, and defensible approaches help you translate legal requirements into clear, actionable steps for your incident response plans.

Key takeaways

- The latest privacy law changes in 2026 and how they affect incident response
- OAIC notification rules including timelines, required information, and common mistakes
- Insights from 2025 enforcement activity and where OAIC is directing attention
- Practical templates and structures for compliant notifications to regulators and affected individuals
- How to protect legal privilege while meeting disclosure requirements
- Strategies for managing OAIC scrutiny during an active incident while keeping investigations on track

Facilitator

Simone Herbert-Lowe

Partner, Clyde & Co

Simone is a partner in Clyde & Co's insurance practice and leads its Australian Cyber team. A recognised expert in cyber risk, privacy and legal liability, she advises on cyber incidents, insurance coverage, professional liability and cyber resilience. With over 30 years' experience across litigation, regulatory response and strategic risk advisory, Simone brings deep insight and practical leadership to this area. Combining sought after expertise in facilitating incident response exercises with the delivery of industry-leading cyber education, Simone's leadership has been recognised through awards for innovation, cybersecurity and ethical business practice.

NEW FOR 2026 LEGAL BACKGROUND BRIEFING

Translate legal requirements into clear, actionable steps for your incident response plans.

SESSION

Crisis Communications & Stakeholder Masterclass

When a breach hits, your first message can decide whether you stay in control or lose the narrative entirely. Matthew Abbott brings twenty years of crisis communications experience across financial services, fintech, retail, and regulatory environments to teach the principles of high-pressure crisis messaging. After nearly a decade leading corporate affairs at ASIC and senior roles at Latitude Financial, Zip Co, and Westfield, he understands the tension between transparency and investigation integrity, regulatory expectations and stakeholder pressure, and the battle between speed and accuracy.

This masterclass focuses on what works in real incidents. You will learn the message structure that supports effective response, how to map and prioritise competing stakeholders, and how to communicate cyber incidents in heavily regulated sectors. The session also fills a major gap in traditional crisis training by adding an internal communications component, including employee notification protocols, HR coordination, and how to prevent staff from triggering a secondary crisis. Case studies from Australian breaches highlight what succeeded, what failed, and why timing determines outcomes.

Key takeaways

- What to say first, second, and third in a cyber crisis and why sequencing matters
- How to map and prioritise stakeholders including media, regulators, customers, employees, and investors
- Templates for effective external communications across all phases of an incident
- Internal communications essentials including staff notifications, HR coordination, and managing internal information flow
- How to create two-way communication so frontline teams feed insights back to incident command
- Lessons from recent Australian breaches and what distinguishes effective messaging
- How to balance transparency with investigation integrity
- Approaches for communicating with regulators while staying in control
- Preparing executives for media and stakeholder engagements
- How to manage journalists and prevent speculation
- How to reduce the risk of employees amplifying misinformation

Facilitator

Matthew Abbott

Corporate Affairs Leader, Ex-Latitude Financial, Zip, and ASIC.

Matthew Abbott is a Corporate Affairs leader with experience across financial services, fintechs, regulation and property, leading communications, government relations, and public policy functions in these sectors. Matthew has held senior Corporate Affairs roles in the listed world at Latitude Financial, Zip Co and Westfield, and spent nearly a decade leading corporate affairs at the Australian corporate watchdog ASIC. He was also an advisor to former treasurer Hon Joe Hockey and started his career as a reporter with the Australian Financial Review. A seasoned strategist known for navigating complex regulatory and public environments, Matthew brings deep expertise in stakeholder engagement, media relations, and crisis communications—skills honed over two decades shaping communications for high-impact organisations.

MASTER THE ART OF CRISIS MESSAGING UNDER PRESSURE

Master Crisis Messaging, Stakeholder Mapping & Internal Response—The Missing Piece in Traditional Crisis Training

SESSION

Cyber Breach Response Workshop

This live simulation places you inside a fast-moving cyber incident where information is incomplete, pressure is high, and every decision affects the outcome. Participants split into Red and Blue Teams and experience the full lifecycle of a breach, from initial detection through to public crisis escalation. Guided by expert facilitators, you will apply technical, legal, and communications frameworks in real time, testing decision-making, coordination, and leadership under stress. The experience mirrors the reality of modern breaches where technical response and public crisis management collide. The workshop closes with a reverse panel debrief session featuring red, blue, and legal leaders to explore lessons learned.

Part 1: Initial Breach Detection and Response

Part 1 focuses on the first hour of the incident. You must decide how to contain the threat, preserve evidence, determine notification triggers, and coordinate legal, technical, and communications workstreams while the breach may still be active. Teams must apply the crisis messaging principles from Matthew Abbott's masterclass to early stakeholder decisions including board briefings, regulator contact, customer considerations, and internal staff communication.

Key takeaways

- First-hour decision-making under uncertainty
- Technical response fundamentals including containment and forensics engagement
- Cross-functional coordination between IT, Legal, Communications, and Executives
- Legal and regulatory triggers with real-time guidance from Simone
- Early stakeholder notification choices and their consequences
- Applying crisis communication principles to early messaging
- Red Team insights into attacker thinking and escalation patterns
- Practising core incident response roles

Legal Lead: Simone Herbert Lowe
Blue Team: Sam Fariborz, David Jones (QLD)
Red Team: Clyde Netto, Thomson Reuters

Part 2: Crisis Communications Challenge Inject

At the start of Part 2, the situation escalates into a full media crisis. Reporters are publishing stories, social channels are spiralling, and stakeholders demand immediate answers. Teams must manage the technical response while simultaneously handling a public-facing crisis. You will apply Matthew Abbott's frameworks for media management, stakeholder alignment, and message architecture in a high-pressure environment.

Key takeaways

- How technical incidents turn into public crises and how to stay in control
- Crafting and delivering holding statements under extreme time constraints
- Managing technical containment while handling competing stakeholder demands
- Navigating pressure from insurers, regulators, boards, customers, and media
- Real-time legal boundaries to protect investigation integrity and privilege
- Applying crisis communication principles to a live incident
- Red Team insights on how attackers exploit confusion
- Understanding when to communicate early and when to hold back

IMMERSIVE TEAM-BASED SIMULATION WITH EXPERT FACILITATION

Scenario pack, company profile, and role briefings provided

SESSION

30-Day Action Plan + Board Reporting Workshop

This is the difference between training and transformation. Most workshops end with inspiration but no implementation, this one ends with your personalized 30-day roadmap. Working with expert facilitators, you'll build actionable plans tailored to your organisation's maturity, resources, and risk profile. You'll develop incident response decision trees, legal compliance checklists, stakeholder communication cadences, technical remediation roadmaps, and critically; board reporting frameworks that translate cyber incidents into language executives and directors understand. This session also addresses a gap most training ignores: how to manage board expectations, reporting frequency, and communication strategies during active incidents.

Speakers

Simone Herbert-Lowe
Partner,
Clyde & Co

Clyde Netto
Regional Head of Technology and Cyber Security, Asia and Emerging Markets,
Thomson Reuters

Key takeaways

- Incident response decision tree: Navigate key decision points with clarity—when to escalate, when to notify, when to engage external support
- Legal reporting checklist: Ensure compliance with OAIC, SOCI Act, ASX disclosure, and cyber insurance notification requirements
- Evidence chain management: Protocols for preserving evidence, engaging forensics firms, and protecting legal privilege
- Stakeholder communication cadence: Who to tell, when, how often, and through which channels—mapped to incident phases
- Technical remediation roadmap: Prioritize fixes, controls, and resilience investments based on risk and feasibility
- Board reporting framework: What boards need to know vs. want to know, how to present technical information to non-technical directors, and sample board questions with answers
- Managing board expectations during incidents: Communication strategies for leadership under pressure—reporting frequency, escalation triggers, and handling board anxiety
- 30-day implementation plan: Your personalised roadmap with specific actions, owners, and timelines for the next month

NEW FOR 2026 - IMPLEMENT YOUR LEARNINGS & CREATE A PERSONALIZED 30-DAY ROADMAP

Interactive workshop with template development and expert coaching

Thomson Reuters™

Thomson Reuters Legal Australia events team is a dedicated team designing and curating some of the most up-to-date, industry leading, and larger-scale events in Australia and New Zealand.

Most of our events are CPD-accredited and offer great networking opportunities for professionals alike in the field of legal, corporate, tax & accounting, and related fields.

Thank you for joining our event! We look forward to seeing you again soon.

FOLLOW US TO STAY UPDATED ON OUR UPCOMING EVENTS!

Upcoming Events

TR Legal Australia Official LinkedIn

Thomson Reuters Events ANZ Official LinkedIn

CYBERSECURITY & BREACH RESPONSE BOOTCAMP 2025

30 October | Melbourne

Produced by

THOMSON REUTERS EVENTS ANZ

Thomson Reuters™

Contact us

Interested in attending, speaking at or sponsoring our future events?
Please contact us to find out more about what we have in store.

Ask me about speaking opportunities

Katie Ardzejewski
Conference Producer ANZ
Thomson Reuters - Asia and Emerging Markets
Mobile: +61 404392572
Katie.Ardzejewski@thomsonreuters.com

Ask me about brand and partnership opportunities

David Lewis
Sponsorship & Delegate Sales Manager, Legal Media Group
Thomson Reuters - Asia and Emerging Markets
Mobile: +61 405 217 138
David.Lewis3@thomsonreuters.com