

# Andrew Karvounaris

## Director in Melbourne

+61 3 9278 1045 / +61 484 066 007

akarvounaris@mcgrathnicol.com



## Qualifications & Memberships —

- Certified Computer Examiner (CCE)
- Bachelor of Business Information Systems (RMIT)
- Diploma Government Investigations
- Cert IV Government Investigations
- Cellebrite Certified Operator and Physical Analyst
- International Association of Computer Investigative Specialists (IACIS)
- Australian Information Security Association (AISA)

As a Director in Melbourne's Technology and Cyber team, Andrew brings over 14 years of experience in Digital Forensics, Incident Response, eDiscovery, Investigations, and Cyber Threat Intelligence. He has extensive expertise in managing complex security challenges across both the private and government sectors and has a deep understanding of incident management, breach response, and compliance, particularly during high-stakes cyber incidents.

Andrew manages Incident Response and Cyber Threat Intelligence engagements nationally, and has built a reputation as a trusted advisor to clients in navigating high-pressure cyber security crises. He oversees the entire lifecycle of incident management, from initial detection and containment to threat eradication and system recovery.

As part of his role, Andrew oversees the collection, analysis, and dissemination of threat intelligence to identify and mitigate emerging risks. This proactive approach helps clients address vulnerabilities before they can be exploited, strengthening their security posture and reducing risk.

Andrew works with clients to navigate crises and advise on future improvements, ensuring they are not only prepared to respond to incidents but also equipped to proactively defend against emerging threats.

## Engagement Experience —

### Cyber Security

- Led and managed the immediate cyber incident response activities (containment and root cause analysis) for various clients that have fallen victim to ransomware attacks or unauthorised access resulting in a loss of access to critical business system and loss of data.
- Acted as an Independent Computer Forensic Expert to investigate unauthorised access to confidential information and intellectual property theft.
- Led and managed demanding legal and regulatory inquiries, including information requests from the Royal Commission into Bushfires and Natural Disasters and ACCC S.155 notices.
- Led engagements to comprehensively overhaul data security through the Data Classification and Data Loss Prevention uplift projects. Andrew managed the creation of robust DLP rules with blocking and implementation of a new, organisation-wide data classification label.
- Contributed to several warrants visits with government agencies to undertake forensic computer analysis. This included taking forensic copies



McGrathNicol



McGrathNicol

## Andrew Karvounaris Director in Melbourne

of electronic devices and analysing the forensic images to identify evidence of fraudulent documents, statements, invoices etc.

- Led and managed a team of Threat Intelligence analysts to oversee the collection, analysis, and dissemination of critical threat intelligence, working closely with stakeholders to identify emerging risks and trends. This proactive approach allows our team to address vulnerabilities before they can be exploited, strengthening our clients' security postures.
- Delivered numerous cyber awareness programs (inclusive of cyber awareness training workshops, tabletop scenarios, development of cyber awareness content and on-going testing of staff awareness) for our clients.