McGrathNicol

Joss Howard

POSITION	Partner	SYDNEY OFFICE
PHONE	+61 2 9338 2640	
MOBILE	+ 61 460 972 700	Level 12
EMAIL	jhoward@mcgrathnicol.com	20 Martin Place
WEBSITE	mcgrathnicol.com	Sydney NSW 2000

Qualifications & Memberships

- Certified Information Systems Security Professional (CISSP)
- Information Systems Security Management Professional (ISSMP)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Management Professional (CISMP)
- Associate of the Australian Institute of Company Directors (AICD)
- Australian Information Security Association (AISA)
- Cyber Leadership Institute (CLI)

Board Roles

- InfoSecAssure, Technical Advisory Board Member

Joss has led teams in delivery of technical, information security and cyber resilience projects for over 25 years. She has held senior security management positions in military, industry and professional services. Joss has advised companies globally, including in the aerospace, defence, finance, government, healthcare, leisure and retail, transport, telecommunication and utilities sectors.

Her professional services career has included working with an extensive number of clients globally, helping to tackle cyber risk and increase security posture. She specialises in assessing security posture, developing strategies, and identifying investments, resources and initiatives to achieve optimal cyber security growth for her clients. Further, Joss advises boards and senior management on initiatives to improve their business resiliency against cyber threats, reduce risks and protect profitability.

As an authentic security professional, Joss' experience is relied upon at the board, senior management and operational level of a business. She is regarded by clients as a 'trusted advisor' and a cyber leader providing genuine insight and innovation on information risk and cyber-security matters.

Joss contributes to the wider security profession with ISACA and mentors emerging security professionals who want to excel and exceed in cybersecurity.

Engagement Experience

Cybersecurity Strategy, Board and C-Level Advisory

- Australian Water Company: Advising the Executive team to develop a five-year strategy based on NIST Cyber Security Framework (CSF), to ensure compliance to cyber security and data privacy regulatory requirements.
- Australian Building Society: Assist senior cybersecurity management on the development of a 5-year cybersecurity strategy, post NIST CSF control.
- Australian Superannuation Company: Board level presentation to demystify cybersecurity, provide tools and mechanisms to discuss cyber risk effectively and increase engagement between the Board and senior technology management.
- Australian Superannuation Company: Board level presentation to provide oversight of Australian Government cybersecurity initiatives, a cyber security analysis of its own operations, and potential threats that it faced.
- Australian Cyber Advisory Organisation: Assisted in the development of a controls framework to provide advice and guidance to Australian small and medium sized businesses, with the objective to improve their cyber resilience posture.
- Global Foreign Exchange Company: Advising the board and executives to design, develop and implement a 3-year cyber security improvement strategy, based on ISO27001 and NIST CSF, to improve its security posture and meet global regulations.

- Papua New Guinean Bank: Advising C level and senior management on the development of a long-term cybersecurity strategy, the restructuring of their cybersecurity department to meet business needs and refresh their cybersecurity policy and procedures. Further work saw me advise on cyber insurance benefits, review of department competency and report findings to senior management.
- UK Household Technology Manufacturer: Define and design the roles and responsibilities for the cybersecurity operations.

Cybersecurity Governance, Risk and Assurance

- Australian Bank: Assess their cybersecurity posture using the SWIFT Customer Security Controls Framework (CSCF), to achieve a position in readiness for attestation.
- Australian Financial Software Company: Assess cybersecurity posture using the SWIFT CSCF, to achieve a position in readiness for attestation.
- Australian Superannuation Company: Assess and re-assess cyber controls to ensure alignment to APRA CPS 234 and provide pragmatic remediation.
- Australian Insurance Company: Assess of cyber and business controls to ensure alignment to APRA CPS 234 and provide pragmatic remediation.
- Australian Data Solutions Company: Assess the physical, information and personnel security controls prior to approval to operate and transfer data with Google.
- Australian Leisure Company: Prior to acquisition, I was engaged to assess and provide a report on an American travel company, to ascertain cyber and privacy risks which could impact the deal.
- Australian Telecommunications Company: Managed a UK, Singapore and UK team to determine control maturity, cyber threats and risks that may affect their 5G infrastructure.
- Australian University: Assess departments cyber control posture based on Center for Internet Security (CIS), to provide gaps and improvement initiatives.
- Global Leisure Accommodation Company: Assess the physical and cyber controls of hotels located in Europe and UK, to determine risks and areas for improvement.
- Global Insurance Company: Assess the cyber control and conduct a data discovery exercise to determine the protection required for its sensitive data.
- Global Private Equity Company: Lead a project team to assess the company’s Australian and European assets cyber security and risk posture, prior to selling.
- Global Communication Solution Vendor: Assess newly acquired business to determine cyber risks, regulatory compliance and cyber control maturity.
- European Smart Meter Manufacturer: Assess the development environments that produced devices for the UK electricity market. The approach was based on UK Government requirements covering the physical, software and hardware development environments and personnel security.
- Global Financial Administration Company: Assess their UK operations cybersecurity posture using the SWIFT Customer Security Controls Framework (CSCF), to achieve a position in readiness for attestation.
- European Airline: Assess the IT and business operations security controls against CIS.
- Papua New Guinean Financial Institution: Assess physical and technical controls against the CIS framework to determine a 3-year strategy with defined initiatives.

Assisted in the development of the Information Security Management System (ISMS) and review of network configuration, to increase cyber resilience maturity.

- UK Government Department Licensing Organisation: Conduct in-depth review of cyber security controls, incident response capabilities and conduct 'red-team' exercise to identify gaps and provide remediation.
- UK Financial Institution: Assess the UK and European business unit cyber security controls against the CIS framework, providing understanding of gaps and remediation. Further, I was engaged to be their virtual Information Security Manager, aiding in the development and implementation of the identified remediation.
- UK Insurance Company: Assess the software departments' compliance to UK Cyber Essentials Scheme and provide detailed report to its Board.
- UK Military Museum: Assess the operations compliance to UK Cyber Essentials Scheme and provide detailed report to its Board.
- UK Independent Boarding School: Assess physical and technical controls against ISO27001 to determine gaps and remediation opportunities.
- UK Food Outlet: Develop cyber risk register and assessment approach for onward management, and presentation of risks to the Board.
- UK Retail: Conduct cyber risk assessment of its business using the Information Security Forum, Information Risk Assurance Methodology (IRAM) and presentation of outcomes to senior management.

Data Privacy

- Australian Recruitment Company: Assess business and cyber controls against GDPR requirements to identify control and regulatory gaps and provide remediation opportunities.
- Global Software Optimisation Company: Assess cybersecurity controls and data privacy processes to ensure compliance to General Data Protection Regulation (GDPR) and regional regulatory requirements. Further, aided in the creation and development of its Mandatory Data Breach Notification policy and presented data privacy policy and GDPR requirements to its staff, to ensure compliance requirements.
- Global Communication Solution Vendor: Assess data privacy processes to ensure compliance to General Data Protection Regulation (GDPR) and presented GDPR requirements to senior management, to ensure compliance awareness.
- Global Commercial Real Estate Services: Identify the data privacy requirements of each of the fourteen countries that it operated in, map those regulatory requirements against GDPR, and conduct an assessment to identify non-compliance and remediation.
- Global Digital Health Platform Company: Create and aid implementation of their information security policy and procedures, to ensure compliance to US health and European data privacy regulations.
- Taiwanese Electronic Telecommunications Component Manufacturer: Assess controls to ensure assurance to Microsoft Supplier Security and Privacy Assurance program.
- UK Motoring Association: Conduced workshops to determine the data lifecycle, consequence of its loss and actions to take to protect sensitive information and comply with UK Data Privacy Act.

Joss Howard

Partner

Cyber Incident Response

- Australian Data Solutions Company: Leading and observing an incident response exercise to validate its capability, policy and playbooks, and providing a detailed remediation plan.
- Australian Utilities Organisation: Leading and observing an incident response exercise to validate its capability, policy and playbooks, and providing a detailed remediation plan.
- Australian Transport Organisation: Leading and observing an incident response exercise to validate its capability, policy and playbooks, and providing a detailed remediation plan.
- Australian Water Suppliers: Leading incident response exercises to validate capability, policy and playbooks, and providing a detailed remediation plan.
- Australian ASX Logistics Provider: Leading and observing an exercise to test the Cyber Incident Response and Crisis Management Teams response capability and validate playbooks to for effectiveness.
- Australian ASX Listed Oil and Natural Gas Production Company: Providing expertise and observing response to incident and to validate playbooks to for effectiveness.
- Australian Superannuation Firm: Leading and observing incident response exercises to validate capability, policy and playbooks to provide detailed reports to increase effectiveness.
- Australian Health Service: Leading and observing an incident response exercise to validate its capability, policy and playbooks, and providing a detailed remediation plan.
- Global Insurance Firm, Australian Operations: Leading and observing an incident response exercise to validate business operations and Cyber Incident Response Team (CIRT) capability, policy and playbooks to provide detailed reports to increase effectiveness.