CYBER
SAFE COUNCIL

SAFEGUARDING COUNCILS WITH COMPREHENSIVE CYBERSECURITY

With cyber attacks increasing in frequency and complexity - we have all witnessed a heightened level of malicious cyber activity in recent years.

Cybercrime can cause financial and reputational damage, disrupt business and essential services, and result in permanent damage to an organisation. In 2021-22 over 76,000 cybercrime reports were lodged - with ransomware the most destructive trend. Ransomware groups are constantly evolving to maximise their impact by targeting the reputation of Australian organisations. In 2021–22, ransomware groups stole and released the personal information of hundreds of thousands of Australians as part of their extortion tactics. The cost of ransomware extends beyond the ransom demands, and may include system reconstruction, lost productivity, and lost customers.

Australian organisations, and even individuals, are also being targeted by malicious cyber actors. Malicious actors persistently scanned for any network with unpatched systems, sometimes seeking to use these as entry points for higher value targets. The majority of significant incidents in 2021–22 were due to inadequate patching.

ABOUT US

KIRRA Services delivers experienced and comprehensive cybersecurity solutions to support your organisation to mitigate cyber security incidents. Our consultants bring over 20 years experience securing Australian government agencies. They have worked to develop and refine methods for detecting and mitigating targeted cyber intrusions of Australian government IT systems and networks.

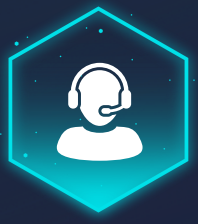
We are also a Defence Industry Security Program 2 (DISP) member with the ability to sponsor security clearances and support organisations to meet DISP cyber requirements.

ASSESS: A comprehensive assessment of the current cybersecurity maturity is undertaken to evaluate the current security practices and identify gaps or vulnerabilities within systems.

MITIGATE: Advanced threat detection including intrusion detection, firewall protection, antivirus and malware. We secure network infrastructure by implementing strong access controls, secure configurations, and regular security audits. Our Incident Response includes real time monitoring, alerts, patching and data protection to address threats and vulnerabilities.

PENETRATION: Penetration testing including controlled security assessments to test and detect vulnerabilities and simulate real-word scenarios to ensure the best possible defence against a cyber threat.

MONITOR: Ongoing monitoring and evaluations to ensure your cyber solution remains at the front of the game and responsive to emerging and evolving cybers threats and compliance requirements.



SUPPORT: Ongoing technical support, including service implementation, configuration, and troubleshooting. Training resources and user documentation and certified cyber training courses and vendor certifications from beginner, intermediate to advanced.

www.kirraservices.com.au/cyber