CYBERSHIELD CORPORATE

Cutting Edge Security Testing Services

Powerful yet precise security testing across your applications, platforms and networks.

The benefits

- Identification and mitigation of technical vulnerabilities via tactical recommendations that quickly improve your security posture and prevent security incidents.
- Identification and mitigation of the process deficiencies that cause technical vulnerabilities via strategic recommendations.
- Identification of vulnerabilities early in the project lifecycle, preventing costly re-work, re-testing and project delays.
- Benchmarking of your security posture against other organisations in your industry sector.

All testing is to a pre-defined set of criteria that we report on, enabling you to benchmark your security posture over time on the same systems or between different systems. We have the ability to test cutting edge technologies as well as the full gamut of commonly deployed hardware and software.

Typical security testing services

External Network Security Assessment

From our cloud based testing laboratory we assess your internet facing services — such as SMTP, WWW, IPSEC and SSL VPN, FTP and DNS — to our pre-defined criteria. Meets and exceeds the typical “network-layer annual penetration test” required by standards such as PCI-DSS.

Web Application Security Assessment

We test your web application to criteria aligned with the security controls that prevent the OWASP Top 10 web application security vulnerabilities. Meets and exceeds the typical “application-layer annual penetration test” required by standards such as PCI-DSS.

Internal Network Security Assessment

We attend your premises with our security testing laptops and test the systems supporting your most critical IT services to our criteria, including client side security — for example, desktop software patching to determine susceptibility to spear-phishing attacks with malware laden attachments.

Wireless Security Assessment

A site survey identifies approved and potentially rogue wireless access points on your WLAN, and whether the WLAN extends outside your premises. We examine configuration settings and test key security controls — encryption, authentication and logging — meeting the PCI-DSS requirement to test for the presence of wireless access points.

CYBERSHIELD CORPORATE

What we test

Assessment Service	Criteria Tested
External Network Security Assessment	DNS, FTP, port scanning, SMTP, version and patch levels, and VPN criteria.
Web Application Security Assessment	22 criteria for authentication, 3 for authorisation, 11 for data security, 10 for data validation, 3 for exception handling and 9 for session management.
Internal Network Security Assessment	Desktop and desktop SOE criteria, internal network architecture, internal management interfaces and internal port scanning.
Wireless Security Assessment	Site survey, wireless authentication, wireless encryption and wireless management interface criteria.

Why CyberShield Corporate

Why do we do this?

We make a difference to the information security of Australians.

How do we do this?

CyberShield Corporate works with government and private enterprise to improve the security of personally identifiable information and help secure financial and non-financial transactions.

What do we do?

We specialise in security management, infrastructure security assessment and web application security testing.

Independent

We have no affiliations with product vendors or system integrators and hence can recommend the best course of action for your organisation without bias.

An understanding of the local market

Australian owned and operated — we understand the size, scale, scope and operations of Australian organisations in both the public and private sector.

Our use of cloud technologies

We use cloud services for all of our business activities in order to break new ground and learn through experience for our clients.