CyberCX

CyberCX State of the Hack - 2020

Inside this report

Introduction

Welcome to CyberCX's 'State of the Hack – 2020' report.

The report provides a snapshot of application security (AppSec) practices across Australia and maps a number of significant AppSec trends. Promisingly, is shows that developers are increasingly incorporating security considerations into the software development lifecycle. There remains room for improvement, particularly with regards to increasing AppSec awareness.

CyberCX conducts over 2500 penetration test each year. The data in this report draws on a sample of 189 web application and web service penetration tests. Is assessing the data we have applied the following criteria:

- Assessed only initial penetration tests[1]; and
- Excluded data from projects shorter than three days.

[1] If a client had already undertaken a CyberCX penetration test we did not include the data.

Statistical Overview

In 2019, CyberCX identified a total of 3,539 vulnerabilities from web application and web service penetration tests.

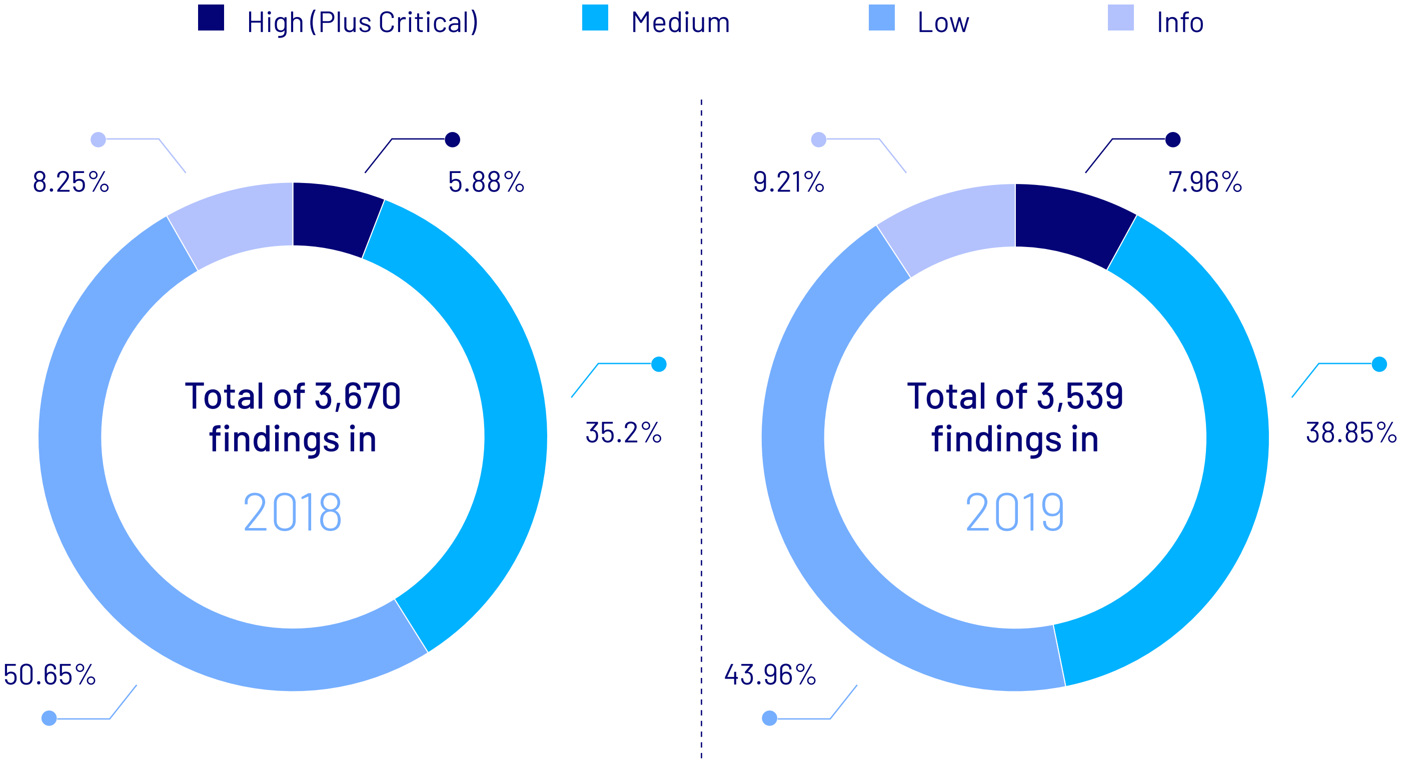
In a positive development, this figure is lower than the 3,670 vulnerabilities identified in 2018. However, it should be noted that the improvement is due to a significant reduction in 'low-risk' vulnerabilities, dropping from 1,859 in 2018 (50%) to 1,556 in 2019 (44%).

The number of 'high-risk' vulnerabilities increased from 216 (6%) in 2018 to 282 (~8%) in 2019. The number of 'medium-risk' vulnerabilities also increased from 1,292 (35%) in 2018 to 1,375 (38%) in 2019.

On average, each penetration test report identified almost 19 vulnerabilities. This is an improvement compared to 2018's average of 21 vulnerabilities identified per penetration testing report.

It is important to note that a report may contain the penetration testing results of more than one web application or web service.

Vulnerability by Percentage



As in 2018, the most common sectors we tested include Government, Technology, as well as Banking and Financial Services.

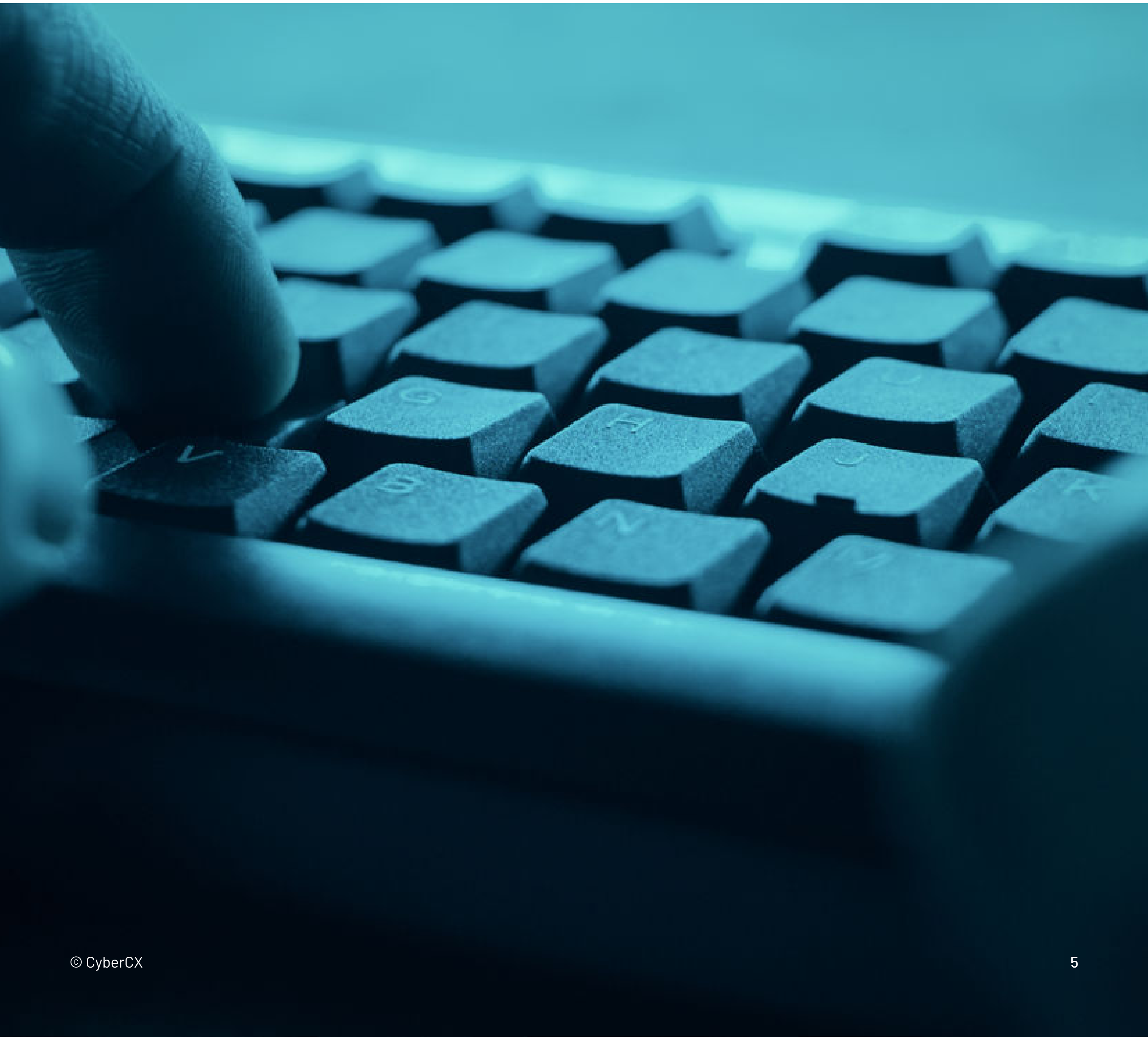
Industry	Total **High**	Total **Medium**	Total **Low**	Total **Info**
Banking and Financial Services	34	182	227	46
Education	14	65	63	9
Food Services	0	5	4	2
Government	61	332	375	72
Health Care	35	150	128	41
Industrial	7	31	27	2
Insurance	2	29	34	12
Other	31	131	153	37
Resources	3	9	15	2
Retail	4	33	46	8
Technology	82	358	423	76
Utilities & Energy	9	50	61	19
Total	**282**	**1,375**	**1,556**	**326**

When comparing the average number of 'high-risk' and 'medium-risk' findings per penetration testing report by sector, the Education, Health Care, and Industrial sectors were found to be the most at risk.

Industry	Average **High**	Average **Medium**	Average **Low**	Average **Info**
Banking and Financial Services	1	6	8	1
Education	2	10	10	1
Food Services	0	5	4	2
Government	1	6	7	1
Health Care	2	9	8	2
Industrial	2	10	9	0
Insurance	0	9	11	4
Other	1	8	9	2
Resources	1	4	7	1
Retail	0	4	6	1
Technology	1	8	9	1
Utilities & Energy	1	6	7	2
Average across all sectors	**1**	**7**	**8**	**1**

Government departments and agencies continue to fare better than private organisations, with lower average numbers of vulnerabilities per report. Even when narrowing down the sectors to those tested most often (Government (~27%) and Technology (~24%)), public sector clients still achieve a lower average number of 'high-risk' findings.

Australian businesses and government departments (both state and federal) are attractive targets for state sponsored attackers and organised crime syndicates. Whilst many penetration tests are conducted in order to assist clients with compliance requirements, there is a noticeable increase in clients seeking broader security assurance. Many large organisations are beginning to realise that achieving comprehensive security requires more than complying with a variety of cyber security standards. Regular penetration testing helps organisations achieve a strong security posture, benefitting all the organisation's stakeholders, including shareholders, employees and customers.



Top 10 Application Security Issues

The 3,539 vulnerabilities identified in 2019 were split into 10 separate categories, closely aligning with the 'OWASP Top 10' categories. It became apparent that 'A6 - Security Misconfiguration' was the top cause of the vulnerabilities we identified in 2019.

Application Security Risk	OWASP 2017 Vulnerability Category
1 – Security Misconfiguration	A6 - Security Misconfiguration
2 – Transport Layer Security	-
3 – Broken Authentication	A2 - Broken Authentication
4 – Sensitive Data Exposure	A3 - Sensitive Data Exposure
5 – Broken Access Control	A5 - Broken Access control
6 – Using Components with Known Vulnerabilities	A9 - Using Components with Known Vulnerabilities
7 – Architectural Weaknesses	-
8 – Insufficient Logging & Monitoring	A10 - Insufficient Logging and Monitoring
9 – Cross-Site Scripting (XSS)	A7 - Cross Site Scripting (XSS)
10 – Injection	A1 – Injection

This is an important reminder that aligning applications with the provisions articulated in the OWASP Top 10 is a good starting point to ensure you develop secure software.

CyberCX identified a large number of vulnerabilities in internet-exposed administrative interfaces, such as WordPress and other Content Management Systems (CMS). Whilst most organisations implement stringent network access controls that limit the exposure of unnecessary TCP or UDP ports, many still fail to consider application layer access control measures, such as limiting internet-exposure of sensitive CMS interfaces.

Too many organisations are failing to adopt Multi-Factor Authentication (MFA) for accessing internet-exposed administrative interfaces. Continued reliance on single-factor authentication, in addition to weak password security, renders such interfaces insecure and makes them attractive targets for attackers.

> *Continued reliance on single-factor authentication, in addition to weak password security, is rendering such interfaces insecure and making them attractive targets for attackers.*

MFA is more important than ever. All internet-exposed interfaces should have MFA configured, especially cloud interfaces. Reliance on single-factor authentication is far riskier, where an attacker only requires one authentication channel (e.g., the login webpage) and valid credentials. Identifying most cloud login pages is relatively straight forward, (e.g., portal.azure.com, signin.aws.amazon.com, etc.), whilst credential theft resulting from breaches is a growing concern.

Password-spraying attacks are increasingly common[2] deployed by both sophisticated and unsophisticated attackers, due in no small part to their low cost. Typically, the simplest way of limiting access to these interfaces is through web application firewall rules or web server configuration.

Sensitive Data exposure is on the rise.
90% *of our reports included at least 1 finding related to SSL/TLS weaknesses.*

In 2019 'A3 - Sensitive Data Exposure' was also a significant cause of many of the vulnerabilities we identified. In most cases, this related to the use of weak SSL/TLS protocols and cipher suites. A staggering 90% of our reports include at least one finding related to this.

Whilst less secure SSL 2.0 or 3.0 appear not to be widely used, migration to the latest versions of TLS is lagging. TLS 1.0 is still the most supported protocol, with apparently slow adoption of TLS 1.2 or 1.3.

The most common reason cited for the continued use of older protocols is that they are suitable for legacy browsers. Organisations seem concerned that end-users are still relying on older browsers, despite evidence to the contrary.

We recommend organisations identify how many clients and end-users still rely on legacy browsers and then take steps to upgrade to TLS 1.3 with a fallback to TLS 1.2.

We identified at least a single SQL injection flaw in ***10%*** *of our reports.*

A number of the reports contained SQL injection (SQLi) vulnerabilities. In total, this finding was identified in just under 10% of our penetration testing reports. Each of these reports may have contained multiple instances of SQL injections as we do not count each instance separately, i.e., we do not count each affected parameter.

For a vulnerability that has been a known problem for over 20 years, we would have expected developers to be adept by now at preventing them.

Another recurring vulnerability is Cross-Site Scripting (XSS). These were identified in 65 or 34% of our reports for a total of 83 findings. The difference between the number of reports and findings is due to the fact that we may including testing of multiple web applications or web services into a single report.

In combination, SQLi and XSS vulnerabilities highlight a lack of input and output validation being incorporated into web applications and web services. Most application frameworks include just such protections but, it would appear that this functionality is not being used sufficiently by developers.

[2] A type of password-guessing attack whereby access to many accounts is attempted using a small set of passwords; also referred to as a horizontal password-guessing attack. Often attackers will gather lists of credentials exposed through breaches and attempt to authenticate using those.

Root Causes

2019 saw changes in the root-causes of vulnerabilities when compared with the previous year.

In 2018 we identified 'configuration flaws' (48%) as the most common root-cause of vulnerabilities, with 'design flaws' (43%) followed closely behind.

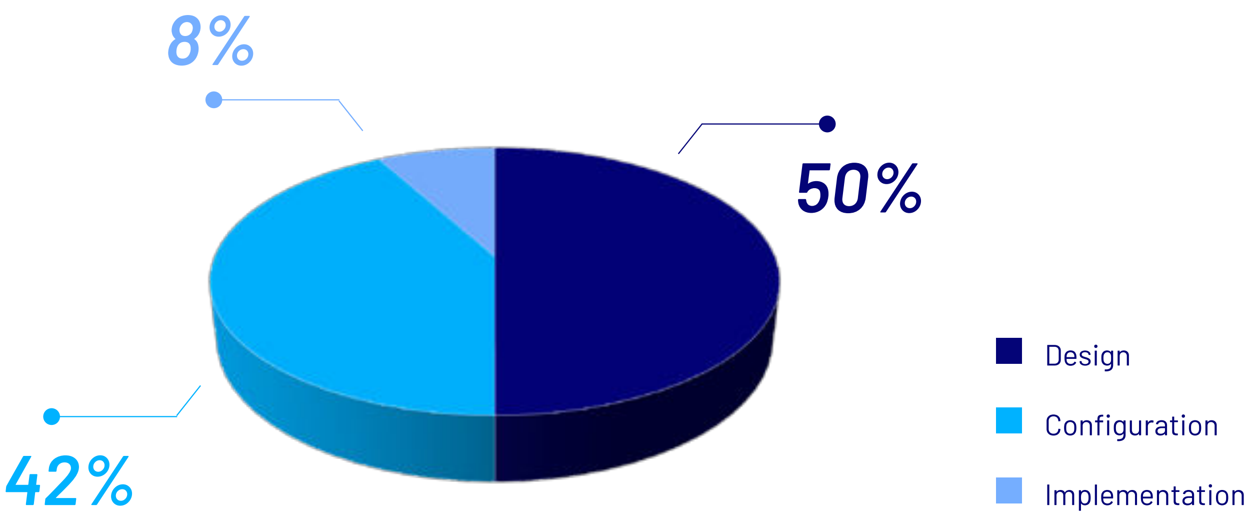
In 2019, these two root-causes have swapped places. 'Design flaws' occurred in almost half the vulnerabilities, whilst 'configuration flaws' occurred in 42% of the cases. 'Implementation flaws' (8%) continue to make a contribution to the root-causes of vulnerabilities.

Design and Configuration flaws trade places

Whilst it is not always possible to ascertain if a flaw was introduced through a design or configuration mistake, both point to the same underlying issue - a lack of design and build standards.

Through the development and enforcement of design and build standards, architects, developers and implementors are reminded to consider any potential security flaws during each phase of the software development lifecycle. A good start is to align with a respected industry standard, such as those from OWASP[3] or CIS[4], customise these off-the-shelf standards to fit your respective business and then enforce and monitor their implementation as often as possible.

Root-causes of vulnerabilities in 2019



[3] The Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) assists development teams by providing a set of requirements that promote the secure development of web applications. https://owasp.org/www-project-application-security-verification-standard/

[4] The Centre for Internet Security (CIS) benchmarks are arguably the leading secure configuration guidelines for a variety of popular products including operating systems, cloud providers, and server software. https://www.cisecurity.org/cis-benchmarks/

Learnings

Investing in security testing early in the development lifecycle pays dividends.

It results in fewer security issues being identified pre-production and raises awareness amongst development teams. Identifying security flaws immediately prior to launching software is significantly more expensive than rectifying security issues during the design and development phases.

In ***58%*** *of reports issued, outdated third-party components made their way into production.*

State of the Hack - six most critical takeaways:

Third-Party Risk

A consistent challenge is the use of third-party components, mainly JavaScript libraries, which are often not kept up to date. This can result in securely developed in-house code being compromised by issues in third-party components developed externally. This may lead to end-users of the application being exposed to unnecessary risk. Software management lifecycles need to include verifying the security of third-party components.

Access Control and Multi-Factor Authentication

Limiting access to administrative interfaces and enforcing MFA go a long way to defending against password-spraying and other brute-force types of attacks. Make sure that access is restricted to all internet-exposed management interfaces and MFA is enabled.

Implement Measures to Prevent Common Weaknesses

Validating user-supplied input is an ongoing challenge for many applications. Utilise the controls provided by modern development frameworks/libraries to combat against common weaknesses such as XSS and SQLi attacks.

Safeguard Data

Organisations need to better protect data in transit and at rest using strong encryption. They also need to comply with the principle of least privilege and minimise the data accessible to the application. Identify the data required by the application and its users to support business processes and remove access to any superfluous data.

Appropriate Configuration of Components

Modern web applications are made up of a number of components with databases, application and content servers, internal and external web services (APIs), firewalls, and load balancers to name but a few. Furthermore, there is an ever-expanding range of cloud SaaS and PaaS services available. As with web applications, it is imperative that organisations develop and enforce configuration and deployment standards for these components, or else the security of the web application will invariably suffer.

Cloud Services

With the ever-increasing adoption of cloud services for business workloads, it is likely that in the future some of the challenges reported on in this report will be resolved. This is good news for organisations that want to focus on providing value to their clients in the quickest and cheapest way possible, with the outsourcing of infrastructure components being one way to achieve this. However, it does come with its own set of challenges, most notably a loss of control. This includes the inability to make changes to component configurations outside of that made available via the client portal, or dictate timelines for improvement or features. The provider’s priorities may not always align with their customer’s needs.

Conclusion

This report into the state of AppSec in Australia in 2020 provides important indicators that help developers, security professionals and executives better understand the extent to which security considerations are being incorporated into applications.

By analysing the common vulnerabilities and security weaknesses identified in this report, organisations can take measures to avoid common vulnerabilities, enhance the security of the software development lifecycle and improve overall cyber security posture.

CyberCX

More Information

For more helpful information, refer to the free resources on the CyberCX website or feel free to reach out to the CyberCX team, who will be happy to answer your questions.

🌐 www.cybercx.com.au

☎ 1300 031 274

About CyberCX

The CyberCX group brings together the country's most trusted cyber security companies to create a comprehensive end-to-end cyber security services offering to Australian enterprise and government.

With a workforce of over 600 cyber security professionals, and a footprint of over 20 offices across Australia and New Zealand, and global presence in Europe and the US, CyberCX offers a full suite of cyber security services.

Our expertise is represented across 8 cyber security practices:

- Strategy & Consulting
- Security Testing & Assurance
- Governance, Risk & Compliance
- Integration & Engineering
- Identity & Access Management
- Managed Security Services
- Digital Forensics & Incident Response
- Training & Education

Led by industry experts and delivered by cyber security specialists committed to their craft, CyberCX represents Australia's best cyber security talent, applying unmatched cyber security expertise to protect and defend Australian organisations from cyber threats.