2025 Nexon Cyber Security Report

7 preventable cyber attack threats facing Australian organisations

nexon™

The **2025 Nexon Cyber Security Report** provides a critical, real-world view of how Australian organisations are being compromised through exploitable attack vectors, and what can be done about it.

The report draws on 126 penetration testing engagements conducted by Nexon Asia Pacific across more than 30 industries between July 2024 and June 2025 to show what is really happening inside local organisations.

We have distilled the research into seven key insights that expose the most common vulnerabilities cyber attackers continue to exploit.

These insights demonstrate that most breaches are not caused by sophisticated adversaries using advanced tactics. Instead, cyber attackers exploit basic and preventable control deficiencies like weak credential hygiene, absent multi-factor authentication enforcement, outdated legacy infrastructure, privilege mismanagement, and human-factor exploitation.

The **2025 Nexon Cyber Security Report** distils insights from 126 penetration tests across more than 30 Australian industries. The results highlight how attackers continue to exploit simple, preventable weaknesses.

of phishing simulations succeeded in capturing credentials

of engagements reached domain admin control

of attacks went completely undetected until reported

Our data shows that even well-resourced organisations continue to leave basic weaknesses unaddressed. Contributing factors include vendor sprawl, lack of integration across tools, and a cyber-skills capacity deficit across the sector that leaves many security teams under-resourced.

Every organisation we tested this year had at least one vulnerability that could have been prevented with stronger foundations. This is not simply a technical challenge, but a business resilience issue.

What's inside

1 Password security: The easiest way in

Weak passwords remain the single easiest way attackers break into Australian organisations.

In our 126 penetration tests this year, low-entropy, predictable, and reused credentials facilitated unauthorised access more often than any advanced hacking technique.

What we found most often:

- "Password123" and other predictable patterns
- Seasonal combinations (eg. Winter2025!)
- Passwords based on company names
- Default or hardcoded service account credentials
- Outdated eight-character minimum policies still in place

Password security: Key findings

of passwords were only 8-10 characters long

1 in 4 organisations reused passwords across accounts

still enforced weak or outdated password policies

Get protected

Nexon Cyber testing showed that the simplest entry points remain the most common. Addressing these basic weaknesses closes off the paths attackers rely on most often.

- Set stronger minimum requirements for passwords
- Remove default or hardcoded service account credentials
- Reduce predictable patterns such as company names or seasonal terms

Stay protected

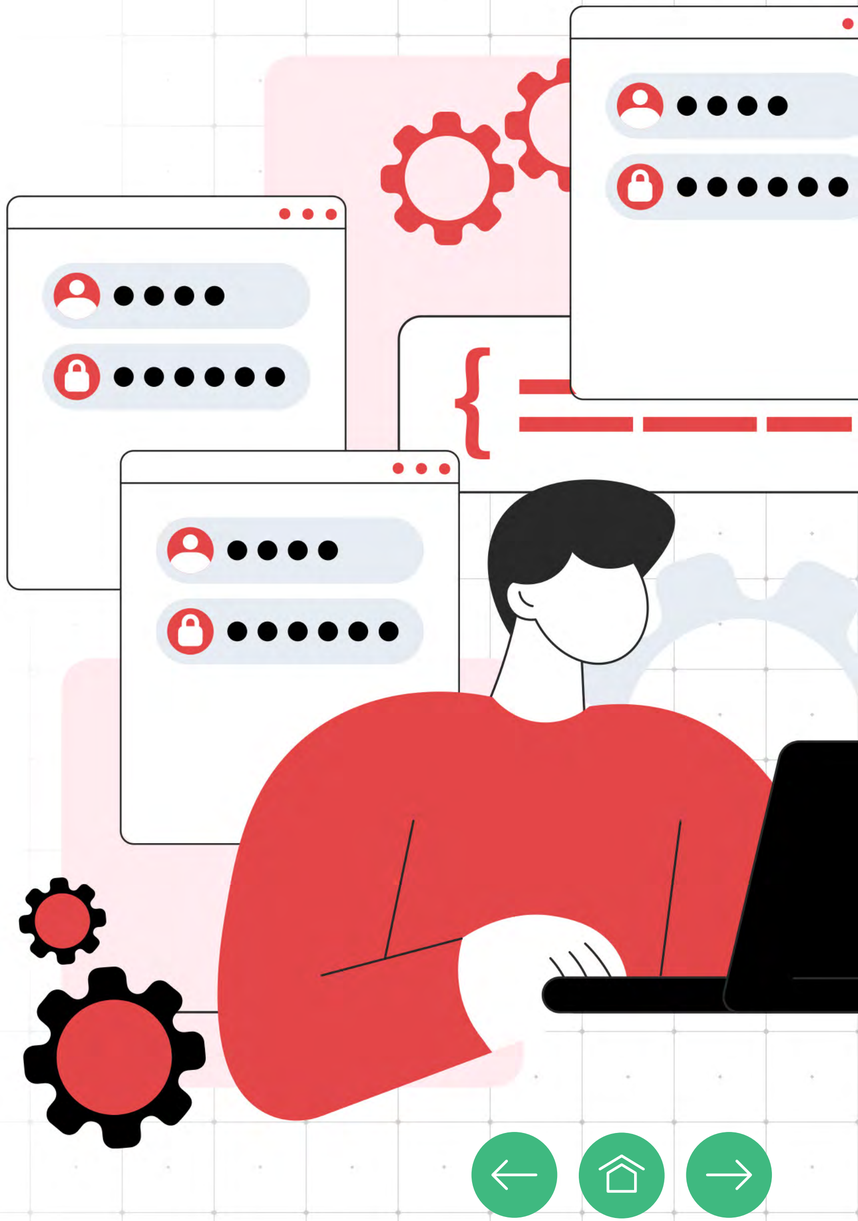
Weak passwords return unless organisations keep them under review. Ongoing monitoring and testing are needed to prevent vulnerabilities from creeping back in.

- Regularly test password policy enforcement and compliance validation
- Monitor for reuse of passwords across accounts
- Audit admin and service account credentials

Don't get caught out

Attackers often escalate quickly once a weak password is compromised. Testing resilience and detection ensures that single account weaknesses don't result in total compromise.

- Incorporate password attacks in penetration tests
- Check how quickly credential-based intrusion attempts are detected
- Review whether a single weak password can escalate to domain added access



2 Authentication gaps: MFA missing where it matters most

Missing or misconfigured multi-factor authentication (MFA) continues to expose high-value accounts.

Even when strong passwords were in place, attackers often found authentication endpoints without enforced MFA or with bypassable challenge flows.

What we found most often:

- Nearly 1 in 10 web apps lacked MFA enforcement
- Cloud admin accounts exempt from MFA
- Executives and service accounts commonly granted MFA exemptions
- Helpdesk processes exploited to bypass MFA resets

9% of web applications had no MFA enabled

5% of perimeter services lacked MFA protection

3% of cloud admin accounts operated without MFA

2% of user accounts were exempted from MFA controls

Get protected

Nexon Cyber data shows attackers frequently gained access where MFA was missing or exempted. Closing these basic gaps is one of the fastest ways to block intrusions.

- Make MFA mandatory for all external-facing logins
- Apply MFA to cloud administration accounts
- Remove exemptions for executives and service accounts

Stay protected

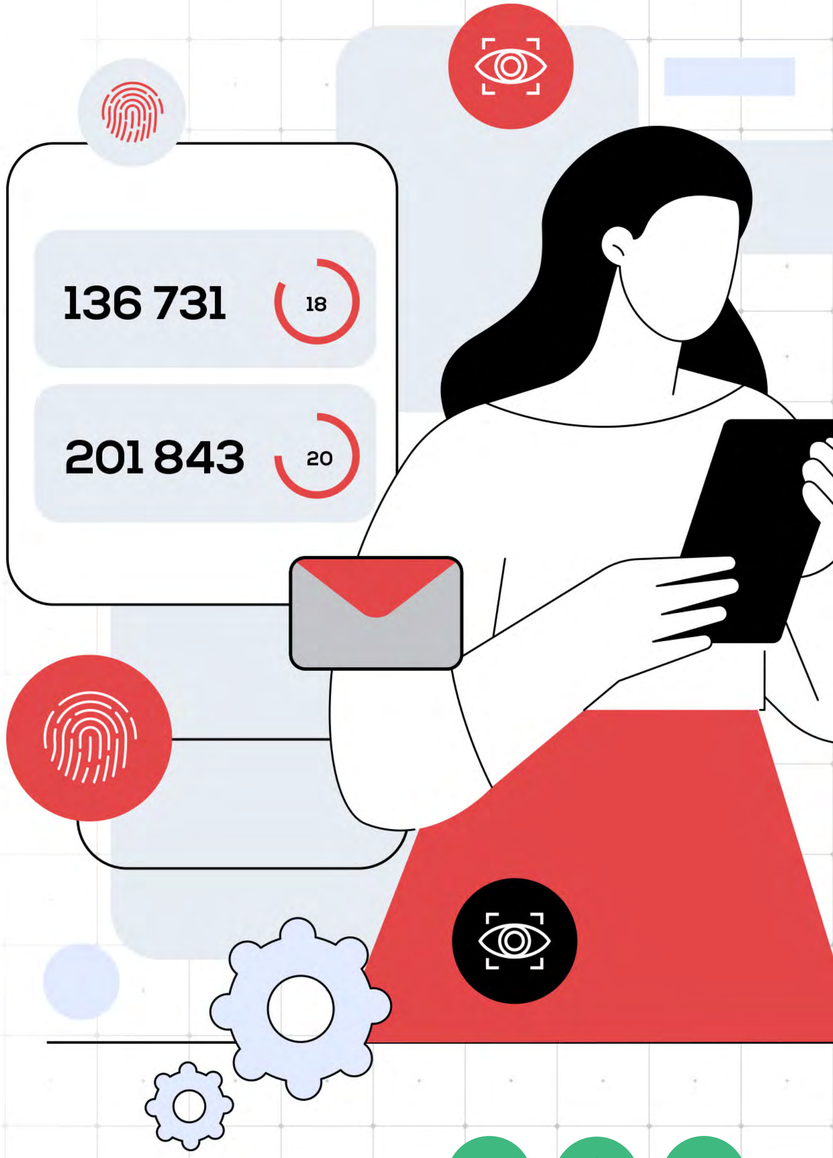
Testing revealed that even where MFA was in place, bypasses exploited misconfigured authentication workflows and exception handling. Regular reviews and validation are needed to keep controls strong.

- Audit MFA coverage and close discovered gaps
- Test help desk processes to prevent MFA bypasses
- Revalidate and rotate MFA devices and tokens

Don't get caught out

Even strong MFA can be undermined by targeted attacks. Testing and advanced methods are required to stop attackers exploiting MFA fatigue or phishing bypasses.

- Detect and block MFA fatigue attacks
- Monitor for phishing-resistant MFA bypass attempts
- Adopt passwordless or phishing-resistant authentication methods



3 Webapps and APIs: Housekeeping flaws drive real-world risk

Everyday mistakes, not complex attacks, are the biggest cause of web and API weaknesses.

Attackers often pieced together small issues, like misconfigured parameters or outdated dependencies, into ways to break in. These simple housekeeping gaps created the majority of real-world risks we uncovered.

What we found most often:

- Security settings left at defaults or misconfigured
- Apps missing essential security control such as HTTP header hardening and input sanitisation
- Outdated libraries still in use
- Upload features allowing disguised malicious files
- Weak or absent web application firewall (WAF) coverage

Webapps and APIs: Key findings

of web applications had at least one security misconfiguration

of APIs lacked critical controls

of tested apps were missing proper security headers

ran outdated or vulnerable components

Get protected

Testing showed that misconfigured parameters and outdated dependencies in web applications were common entry points. Addressing these basic issues removes the majority of exploitable gaps.

- Enforce secure default configurations across apps
- Patch outdated libraries and components
- Deploy and maintain WAF protection on external apps

Stay protected

Findings highlighted that new risks appeared whenever apps were updated or extended. Continuous checks and secure development practices are needed to keep systems hardened.

- Embed security testing in development pipelines
- Conduct regular vulnerability scans of web-facing apps
- Train developers to avoid insecure coding patterns

Don't get caught out

Attackers often chained smaller flaws together to achieve compromise. Simulated attacks and advanced monitoring showed how these combinations could be identified before real exploitation.

- Use penetration testing to simulate chained attack scenarios
- Monitor API telemetry for anomalous behaviour and abuse patterns
- Apply zero-trust access to sensitive APIs and endpoints

4 Human factors: Cyber attackers target people

Phishing and social engineering were the most reliable ways cyber attackers achieved initial access during simulations.

Once attackers got in through people, insufficient internal access controls and network segmentation made escalation easy. And many of these attacks went undetected until our team reported them.

What we found most often:

- Staff entered details into fake login pages sent by email
- Employees revealed sensitive information over the phone
- Helpdesks reset accounts without full identity checks
- Flat networks and weak service account credentials enabled rapid escalation
- Failed login attempts and reconnaissance scans often went unnoticed

of phishing attempts in red team exercises gained credentials

of engagements escalated to domain admin within days

of simulated attacks went undetected by monitoring teams

of reconnaissance scans triggered no alerts

Get protected

Nexon Cyber testing showed that phishing and social engineering were the most reliable ways in. Stronger access rules and removing common weak points reduce this exposure.

- Require two-factor logins for all accounts
- Remove shared service accounts
- Apply network segmentation to restrict lateral movement

Stay protected

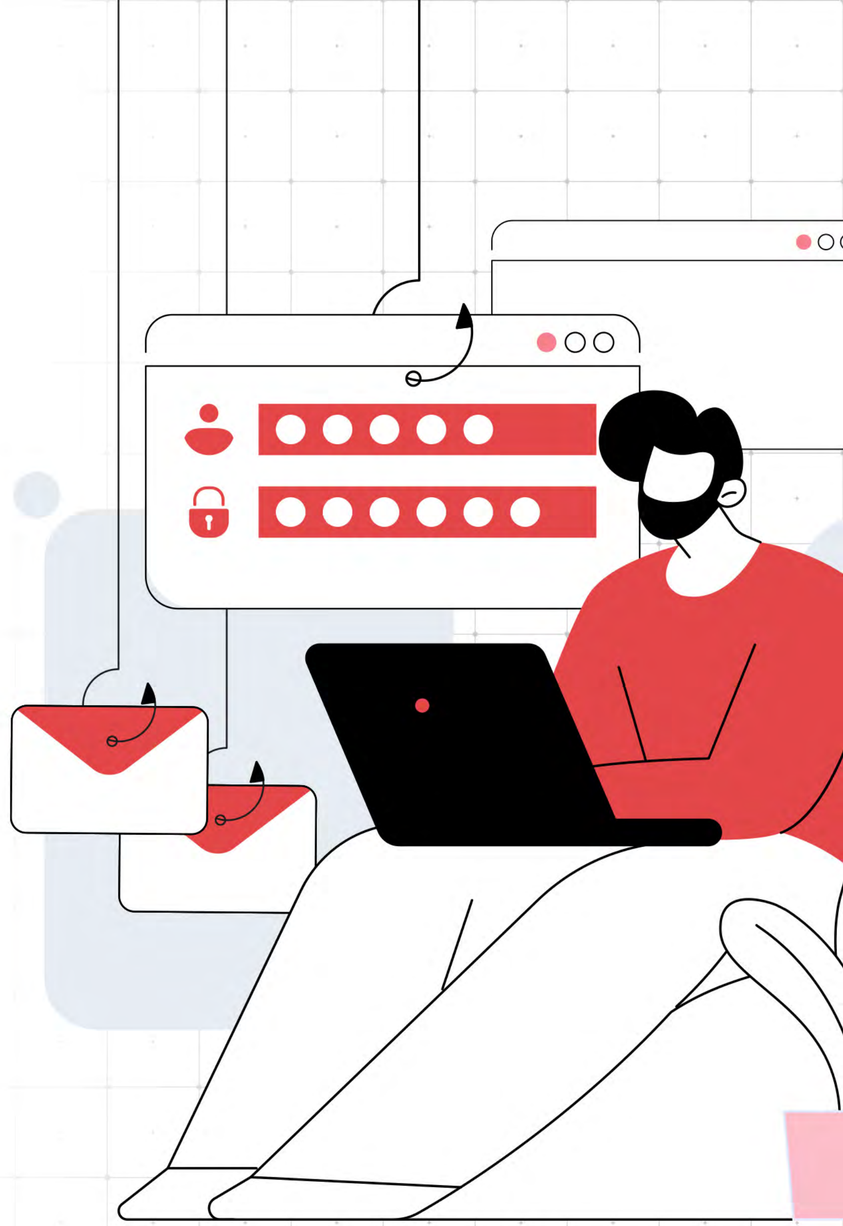
Human weaknesses reappeared without consistent reinforcement. Regular training, refreshed processes, and tuned monitoring are needed to keep attackers out.

- Run phishing simulations and targeted training
- Refresh helpdesk procedures to stop identity bypasses
- Test and adjust detection and alerting rulesets

Don't get caught out

Even with strong basics, social engineering still succeeded at a high rate. Advanced testing and detection methods give organisations the chance to spot and stop attacks earlier.

- Deploy phishing-resistant authentication methods
- Run purple team exercises to test detection and response
- Use analytics to detect anomalous user activity



5 External networks: Perimeters stronger but still exposed

Fewer direct break-ins happened at the perimeter, but simple methods like weak passwords and missing two-factor logins still let attackers in.

In many cases, just one overlooked system was enough to give attackers access.

What we found most often:

- Attackers guessed common or reused passwords on VPNs and email portals
- Internet-facing services running without two-factor login protection
- Outdated or weak website encryption still in use
- Older applications exposed without updates
- Misconfigured firewalls or portals left unnecessary openings

Get protected

Penetration tests showed fewer direct perimeter break-ins, but weak authentication controls and unpatched perimeter assets still created openings. Closing these basics significantly reduces exposure.

- Require two-factor logins for internet-facing systems
- Apply updates quickly to exposed applications
- Review firewall and portal settings regularly

Stay protected

Perimeter systems were found to change often, creating new weaknesses. Ongoing scans and monitoring are needed to catch new exposures as they appear.

- Run routine external vulnerability assessments and attack-surface mapping
- Monitor for repeated failed login attempts
- Maintain an up-to-date inventory of accessible systems

Don't get caught out

Determined attackers continued to probe perimeters. Continuous monitoring and testing makes it harder for them to succeed and reduces reliance on any single barrier.

- Add perimeter systems to 24/7 monitoring
- Include credential stuffing and brute-force simulation in red team exercises
- Adopt zero-trust practices to contain breaches

External networks: Key findings

5% of external-facing services had no two-factor login

8% of organisations had weak or outdated encryption

Multiple cases of unpatched or outdated applications exposed online

6 Internal networks: Flat networks give attackers the keys

Once attackers got inside, they often found networks that were wide open.

Once attackers got in through people, insufficient internal access controls and network segmentation made escalation easy. And many of these attacks went undetected until our team reported them.

What we found most often:

- Outdated or insecure protocols (eg. NTLMv1 and SMBv1) still in use
- File shares with sensitive information open to broad access
- Networks with no separation between user devices and critical servers
- Service account credential reuse and weak authentication controls
- Cleartext passwords found in configuration files

Internal networks: Key findings

of internal tests showed missing safeguards for common services

still relied on insecure legacy protocols

had flat, unsegmented networks

exposed sensitive data in shared drives

of internal breach simulations ended with domain admin control

Get protected

Findings showed that once attackers were inside, flat network topology and inadequate access control mechanisms made escalation easy. Basic safeguards sharply reduce the ability to move freely.

- Disable outdated protocols like NTLMv1 and SMBv1
- Limit access to shared drives with sensitive data
- Strengthen password policies for service accounts

Stay protected

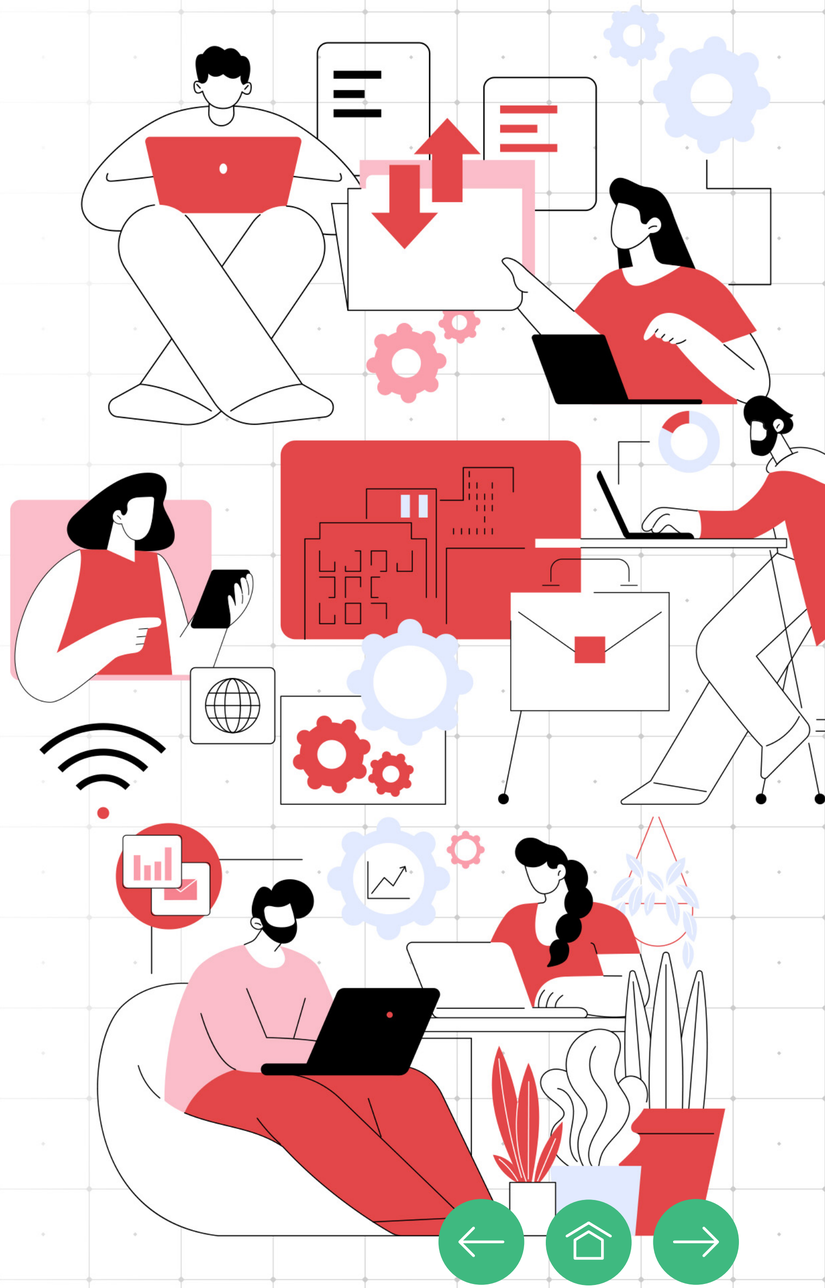
Without regular reviews, insecure protocols and poor access rules persisted. Ongoing audits and monitoring are needed to catch reintroduced weaknesses.

- Audit internal systems and services regularly
- Monitor login behaviour across the network
- Rotate and review service account credentials

Don't get caught out

Tests showed that attackers could escalate to domain admin in most internal compromises. Segmentation and privilege models help contain the impact and limit full control.

- Segment networks to separate users from critical systems
- Apply tiered privilege models for administrators
- Test escalation paths with simulated attacks



7 Cloud misconfigurations: Small gaps create big risks

Most cloud breaches came down to insecure default configurations, not advanced attacks.

Excessive permissions, poor login controls, and dangerous defaults leave sensitive data and accounts exposed in many environments.

What we found most often:

- Cloud services left running with default settings
- Admin accounts exempt from two-factor logins
- Legacy authentication methods still enabled
- Users and apps granted more permissions than needed
- Files and folders shared too broadly outside the organisation

Cloud Misconfigurations: Key findings

6% of cloud setups left unsafe default settings in place

4% used outdated or weak login methods

3% of cloud admin accounts had excessive privileges

2% of user accounts had no two-factor login

Get protected

Nexon Cyber testing found that many cloud breaches came down to unsafe defaults and weak access rules. Setting stronger baselines will quickly close these gaps.

- Enforce two-factor logins for all cloud accounts
- Block legacy login methods such as basic authentication
- Apply least-privilege access to users and apps

Stay protected

Cloud environments changed rapidly, and permissions often drifted from intended settings. Regular reviews are needed to keep access under control.

- Audit user and app permissions on schedule
- Review external file and folder sharing
- Monitor for anomalous authentication events and policy violations

Don't get caught out

Even small gaps in cloud setups were exploited for major impact. Advanced policies and continuous testing helped prevent subtle misconfigurations from escalating.

- Use conditional access policies for risky locations or devices
- Apply continuous monitoring for abnormal account activity
- Validate cloud security through adversarial red team simulation and configuration drift assessments

Your roadmap: Turning insights into action

The seven insights in this report highlight where Australian organisations are most exposed: credential hygiene issues, incomplete MFA enforcement, insecure web application architecture, human error, perimeter gaps, flat internal networks, and cloud misconfigurations.

Each insight points to specific failings, but taken together, they tell a bigger story. Most breaches are not caused by advanced attackers but by simple, preventable vulnerabilities that appear across every layer of the environment.

This roadmap brings those insights together into a single, staged plan. Follow these steps to address each of the seven risk areas in a structured way to build stronger foundations, embed continuous monitoring, and proactively strengthen resilience over time.

Get protected

Testing revealed that basic weaknesses were responsible for the majority of breaches. Addressing passwords, MFA, and misconfigured systems closes off the simplest and most frequent ways attackers gain entry.

- Enforce stronger password policies and remove default credentials
- Apply MFA consistently, including for cloud admin and service accounts
- Verify that identity and access management controls are configured correctly and remain consistent with security policies and compliance standards

Nexon Cyber: Essentials

For organisations starting their security journey, our Essentials tier delivers baseline protection,including MDR and email protection, and two-hour incident response. It ensures the basics are in place before complexity is added.

Nexon Cyber: Advanced

Our Advanced tier provides continuous protection with 24/7 SOC monitoring, security infrastructure management, XDR and email protection, and a two-hour incident response retainer. It gives growing organisations faster detection and response, reducing the risk of undetected compromise.

Nexon Cyber: Premium

Our Premium tier delivers comprehensive coverage including 24/7 SOC monitoring, security infrastructure management, XDR and email protection, vulnerability and identity management.

Stay protected

Findings showed that weaknesses often returned if controls were not reviewed. Continuous monitoring and regular testing make the difference between quick detection and undetected compromise.

- Monitor internet-facing systems and enforce encryption standards
- Patch outdated web apps and components, and secure configurations
- Conduct regular vulnerability audits of internal systems to identify and remediate potential risks.

Don’t get caught out

Penetration testing confirmed that attackers escalated quickly once inside. Advanced validation and proactive improvements ensure single gaps do not turn into full control of the environment.

- Run regular phishing simulations and strengthen helpdesk procedures
- Test cloud configurations, enforce least privilege, and review external sharing
- Use penetration testing and red/purple team exercises to validate defences
- Virtual CISO provides expert security leadership, guiding strategy, compliance, and risk management without the cost of a full-time executive resource.

Go the extra mile with layered services

You can extend protection at any stage by adding extra cyber protection services such as vCISO, staff training and awareness programs, or specialised penetration testing – available as optional add-ons at an additional cost.

Building resilience in 2026 and beyond

The **2025 Nexon Cyber Security Report** confirms what our teams see every day: attackers don't need sophisticated tactics when the basics are still left undone. Weak passwords, missing MFA, unpatched systems, and human error remain the easiest paths into Australian organisations.

Across 126 penetration tests in 30+ industries, every organisation we examined had at least one gap that could have been prevented with stronger foundations. For leaders, this is both a warning and an opportunity.

The warning is clear: The gaps are real, and attackers continue to exploit them.

The opportunity is just as important: These weaknesses can be fixed with a structured, staged approach.

By getting the basics right, embedding continuous monitoring, and strengthening against advanced threats, organisations can move from exposed to resilient in a matter of months, not years.

Cyber resilience is not an abstract goal. It's an organisation-wide imperative that underpins trust, continuity, and growth. The next step is to act.

Glossary

Anomalous authentication: Unusual or suspicious login activity that deviates from normal user behaviour.

API telemetry: Data collected from application programming interfaces (APIs) to monitor usage, performance, and potential security threats.

Attack-surface mapping: The process of identifying and analysing all internet-facing systems, applications, and entry points that an attacker could exploit.

Configuration drift assessments: Reviews that detect and correct unintentional changes to system or cloud configurations.

Control deficiencies: Weaknesses or failures in security measures that reduce an organisation's ability to prevent or detect cyber threats.

Credential hygiene: The practice of maintaining strong, unique, and well-managed passwords or authentication credentials.

HTTP header hardening: Securing web applications by setting HTTP response headers that limit exposure to common web vulnerabilities.

Least-privilege access: A security principle where users and systems are granted only the minimum access rights necessary to perform their functions.

Low-entropy: Describes passwords or encryption keys that are predictable or easy to guess because they lack sufficient randomness.

Penetration testing: A controlled simulation of cyberattacks designed to identify exploitable weaknesses in systems, networks, or applications.

Privilege mismanagement: Improper assignment or oversight of user access rights, often leading to excessive or unnecessary administrative privileges.

Purple team: A collaborative exercise combining red team (attack) and blue team (defence) activities to improve overall detection and response.

Red team: A group that simulates real-world cyberattacks to test an organisation's ability to detect, respond to, and contain threats.

Take the next step with Nexon Cyber

Request a penetration test today to identify exploitable vulnerabilities in your security architecture and don't get caught out against the most common cyber threats.