DIVISION 5

An Annual Industry Report

State of Cyber
Education 2026

With over 2,200 findings across hundreds of Australian organisations, learn about the cyber security posture of the education sector.

INSIDE THIS REPORT

CONTENTS

DIVISION 5

A sector with clear room to improve.

Education has become one of the most consistently targeted industries in Australia. Sensitive information, multiple identity profiles, legacy infrastructure, and tight budgets combine to create a unique threat surface.

"Our Assurance team has carried out penetration tests, red team engagements, and attacker simulations for schools, TAFEs and universities across Australia.

What stands out across every engagement is how fixable the core issues are. The organisations making the most progress aren't necessarily the ones with the biggest budgets, they're the ones with visibility into what actually matters and a repeatable process for addressing it. That's what this report is built around."

Joshua Riesenweber

Director of Research - Division 5

The figures.

A snapshot of the dataset behind this report, including the testing engagements, organisations, and findings that shape the observations in the pages ahead.

2,249
findings analysed across all engagements

36.5%
of education findings rated High or Critical

37%
of findings relate to credentials and lateral movement

22.9%
of education institutions with at least one critical finding

Education vs. other industry.

We compared the average number of critical and high-severity findings carried by an education institution against the average across our client base.

All clients (avg)

6 Critical & high findings per engagement

Education sector (avg)

7 Critical & high findings per organisation

Education environments carry a heavier load of serious findings than most industries we work with, which means there's also more room to make meaningful progress. Understanding where the gap sits is the first step to closing it.

The vulnerabilities we found.

Ten findings reoccur in the education dataset. They speak to foundational controls, and they are a similar group of issues we identify regularly.

TOP 10 - EDUCATION

Vulnerability	AVG RATING
01 Insecure Domain and Local Password Policies in Use	8.3
02 Transport Layer Security Configuration Weaknesses	2.3
03 Insufficient Network Segregation	7.7
04 Systems Missing Software Updates	8.2
05 Least-Privilege Administration Model Not in Use	6.8
06 Service Accounts Susceptible to Kerberoasting Attack	6.5
07 SMB Signing Not Enforced	2.7
08 Environment Susceptible to DHCPv6 Spoofing	7.4
09 LDAP Signing Not Enforced	7.2
10 Information Disclosure Through HTTP Response Headers	1.7

For Comparison

Across our broader client base, the most common findings tilt toward web application and surface-level configuration issues. The education sector looks quite different.

TOP 10 - AUSTRALIA

Vulnerability	AVG RATING
01 Transport Layer Security Configuration Weaknesses	2.3
02 Transport Layer Security Configuration Does Not Conform with Better Practice	2.3
03 Application HTTP Security Headers Do Not Conform with Better Practice	2.3
04 Information Disclosure Through HTTP Response Headers	1.7
05 Information Disclosure via Verbose Error Messages	3.1
06 Application HTTP Security Header Weaknesses	2.3
07 Insufficient Network Segregation	7.6
08 SMB Signing Not Enforced	3.2
09 Outdated Client-Side JavaScript Libraries in Use	1.2
10 Insufficient Password Security Requirements	4.1

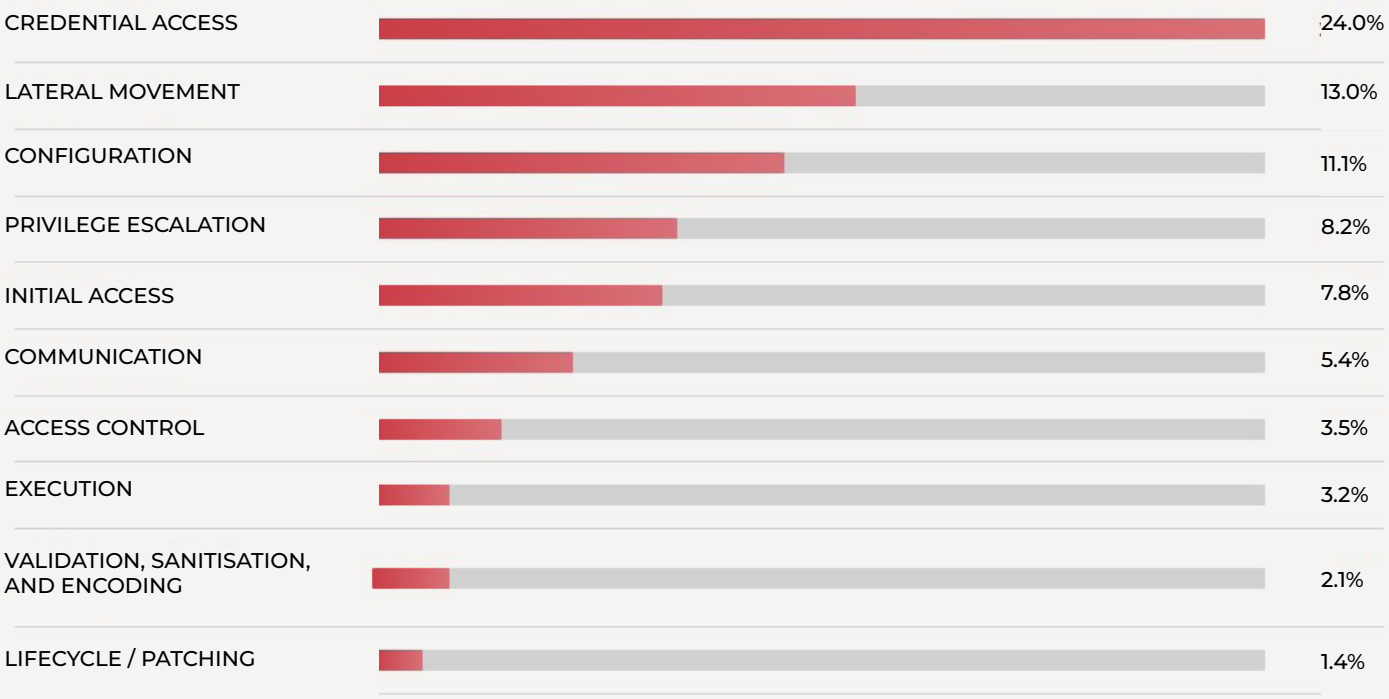
How serious is what we're finding?

Of every 100 findings we report inside an education environment, more than 4 in 10 are rated High or Critical.

The combined 36.5% Critical/High share, paired with an average of 7 such findings per institution, places education materially above our cross-sector baseline of 6.

07 / WHERE THE ISSUES LIVE

Credential Access and Lateral Movement together account for 37% of every finding raised in an education environment, the clearest signal that post-foothold attacker behaviour is where these institutions are most exposed.



Bars scaled relative to Credential Access (24.0%). Categories below 1% omitted for clarity.

08 / THEMES

Three things we keep seeing.

PATTERN ONE

Identity gaps

Least privilege, password policy, and service accounts appear repeatedly in the top ten. In nearly every internal engagement we ran this year, domain compromise was achievable from a standard user foothold (usually within hours, not days).

PATTERN TWO

Flat networks

Insufficient network segregation appears as the second most common finding, and again at #5 across all sectors. Environments with even coarse network segmentation give their teams a meaningful advantage. It doesn't require a full network redesign to start seeing the benefit.

PATTERN THREE

Patching currency

Missing software updates carry high severities in education environments. The challenge is rarely awareness; it is ownership, change windows, and end-of-life systems that are challenging to decommission.

09 / THE YEAR AHEAD

Five priorities for FY26/27.

01

Give your team clarity on who can access what and stop attackers.

Apply role-based access controls and enforce least privilege across every account tier. Limit who can access what, remove standing privileged access wherever possible, and ensure administrative accounts are scoped to their function.

02

Segregate the network.

Even coarse segregation dramatically increases the cost of lateral movement. Pair with east-west firewalling between zones and a clear policy for what's allowed to talk to a domain controller and sensitive systems.

03

Modernise the password and authentication baseline.

Move to passphrases, enforce MFA on all admin and remote access, retire Kerberoastable service accounts to gMSAs where possible, and audit privileged group memberships regularly.

04

Retire SMBv1 and enforce signing on SMB and LDAP.

These three findings appear collectively more than 120 times in our education dataset. They are well-understood, well-documented, and fixable with policy changes.

05

Adopt a measured, repeatable assurance cycle.

Annual penetration testing, supported by regular validation against the controls above, gives leadership a defensible record of progress against the same metrics used in this report.

10 / ABOUT THE DATA

Transparency about how we tested,

Scope

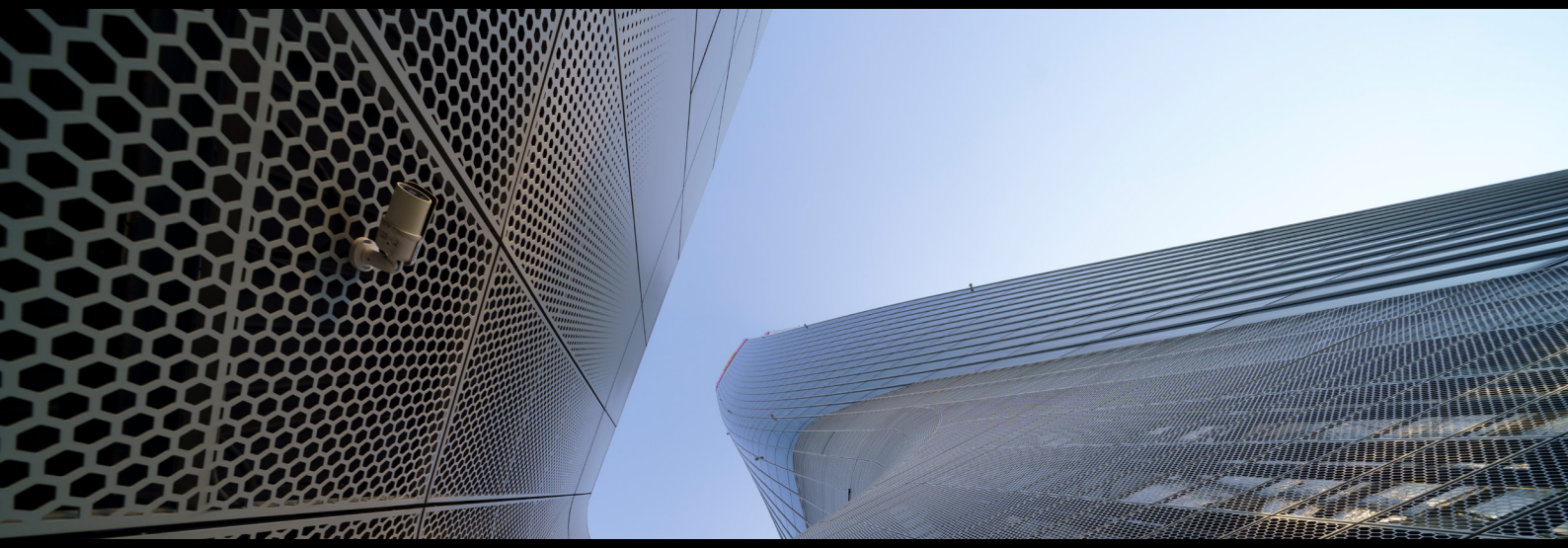
2,249 individual findings drawn from penetration tests, internal infrastructure reviews, and web assessments delivered by the Division 5 Assurance team across calendar year 2025. Education subset: institutions across primary, secondary and tertiary.

Severity Rating

CVSS v3.1 base scores combined with environmental context applied by the consultant. Critical (9.0–10.0), High (7.0–8.9), Medium (4.0–6.9), Low (0.1–3.9), Informational (0.0).

What's not in here

MDR telemetry, incident response data, and findings from engagements where clients have asked us to suppress sector or finding-level disclosure. No identifying institution data is included anywhere in this report.



CONTACT

division5.io

+617 3067 8865

contact@division5.io

155 Wharf Street, Brisbane, Queensland