EXTERNAL PENETRATION TESTING FOR EDUCATION

ALLIANCE BUSINESS TECHNOLOGIES

Are Your School's Digital Doors Unlocked?

In today's connected learning environments, schools rely heavily on cloud platforms, remote access tools, and digital communication systems. But with every new technology comes a new entry point for cyber attackers and unlike large enterprises, most schools don't have a dedicated cybersecurity team monitoring threats around the clock.

This gap in resources is being exploited - education is now the most-breached sector in Australia, accounting for over 33% of all reported data breaches in 2023 (OAIC). Many of these attacks begin with exposed systems like email servers, VPNs, or public websites that schools may not even realise are visible to the internet. Add to that password reuse, oversharing, and low awareness among students and staff, and the risks compound quickly.

The consequences? Disrupted learning, compromised data, and costly recoveries often without warning.

Introducing External Penetration Testing

External Penetration Testing is a practical, non-invasive way for schools to uncover hidden vulnerabilities in their internet-facing systems - before cybercriminals can exploit them. Using advanced automation technology, this service tests real-world attacks to expose weaknesses in your school's digital perimeter.

It's a proactive and affordable approach to strengthening your defences - without disrupting your internal systems or day-to-day operations - to help you:

- Identify vulnerabilities attackers are actively scanning for
- Receive evidence-backed reports showing what could actually be breached
- Prioritise remediation efforts by focusing only on the most exploitable risks
- Reduce reputational, operational, and financial risk from data breaches or ransomware events

Whether you're preparing for compliance, responding to increased cyber insurance scrutiny, or simply taking the first step toward stronger cybersecurity, this is an ideal place to start.

What it covers

A fully automated test of your school's publicly exposed systems.

Internet Reconnaissance
Discovers everything linked to your school's digital footprint from exposed systems and DNS entries to staff email addresses and forgotten third-party tools. This helps you build an accurate inventory of what's publicly accessible.

Real-World Exploit Evaluation
Goes beyond simple detection by safely testing known exploits against your systems. This means you're not just told what might be a risk you're shown what *can actually* be breached.

Dark Web Monitoring
Checks whether school credentials or staff logins have been exposed on the dark web or other criminal sources, helping you stay ahead of identity-based threats.

Evidence-Based Reporting
Every finding is backed by proof so your IT team knows exactly what to prioritise, and your leadership team understands what's at stake.

Recurring Testing Options
Run tests quarterly or monthly to maintain an up-to-date understanding of your risk exposure and demonstrate continuous improvement over time.

Executive-Level Summaries
Reports are written for both technical and non-technical audiences making them ideal for school boards, compliance reviews, cyber insurance renewals, and funding submissions.

Why This Matters for Your Institution

External Penetration Testing provides a practical, low-impact way to take control of your risk exposure:

- No access required - testing runs securely without disrupting operations.
- Clear, prioritised reporting for both IT teams and school leadership.
- Supports compliance with Essential 8, ISO 27001, NIST, and similar frameworks.
- Strengthens cyber insurance submissions and risk assessments.
- Provides measurable evidence for IT uplift and funding applications.
- Helps identify what's exposed, what's at risk, and what to fix first.

Whether you're laying the foundation or building on existing controls, this service is a smart and credible first step.

About Alliance Business Technologies

Alliance Business Technologies (ABT) supports schools, universities, and diocesan networks across Australia with tailored cybersecurity solutions designed for the education environment. Our team delivers penetration testing and actionable insights without disrupting teaching or operations.