Article

Feb 2026

Major identity risk facing Australian universities

The greatest cybersecurity threat facing Australian universities right now isn't ransomware or system failures, but identity compromise - the unauthorised use of legitimate accounts to access sensitive systems, student data, payroll, and research. Attackers no longer need to breach firewalls as they use trusted accounts, making detection more difficult and response slower. This type of access can enable financial fraud, intellectual property theft, and disruption to core operations.

Oliver Baverstock
SOC Team Lead

Email oliver.baverstock@waterstons.com

Why Australian universities are at risk

Universities are open, collaborative institutions by design. They manage large cloud-based environments connecting staff, students, and research partners, have frequent turnover of students, contractors, and visiting academics, and often have decentralised IT management across faculties and research groups

All the while, Australian universities hold high-value assets including defence-adjacent research, energy and medical innovations, and emerging technologies – all of which is very attractive to criminals and state-aligned actors.

Current threat landscape

The main issues facing higher education in Australia are:

- **Targeted phishing and email fraud** are increasingly sophisticated, tricking staff into giving access to accounts.
- **Financial fraud through invoice manipulation** continues to impact university finance operations.
- **Research data theft** occurs quietly, often without triggering alarms.

Incomplete use of multi-factor authentication and outdated login systems also makes it easier for attackers to exploit these weaknesses.

Key gaps in university defences

Many universities have perimeter-focused security, but often high-risk accounts are not fully protected, access privileges are not regularly reviewed, staff and students are not consistently trained on account security, and response plans don't focus on misuse of legitimate accounts. These gaps create open doors for attackers to not only enter, but navigate freely throughout an IT infrastructure.

What you can do strategically

- **Protect high-risk accounts**

Provide hardware security keys to senior administrators, finance leaders, and researchers handling sensitive IP.

- **Strengthen access for all other staff and students**

Use mobile-based authentication apps to secure accounts without adding friction.

- **Review account privileges and lifecycle processes**

Ensure staff and student accounts are deactivated promptly when no longer needed.

- **Monitor and respond proactively**

Treat suspicious account activity as a priority and test response plans regularly.

- **Invest in awareness and culture**

Educate staff and students to recognise phishing attempts and report unusual activity.

As with all cyber security, identity compromise represents a board-level risk - it can affect research integrity, finances, and reputation, without causing obvious disruption.

University leaders should focus on:

Detection speed: How quickly can misuse of access be identified?

Containment: How effectively can the issue be isolated before causing damage?

Prevention: Are the most critical accounts protected with the strongest authentication?

If your university wants to understand more about where your security weaknesses are, we can help! Get in touch at oliver.baverstock@waterstons.com.au