Cybersecurity is a TEAM Sport

Cybersecurity isn't about going it alone. We need and should cooperate at least wihtin our sector, if not much more broadly.

by Vito Forte
Director & CIO
Edith Cowan University

HE Sector in Australia

In 2020, **1,470,865** students studied at Australia's 39 comprehensive universities. Of these, 71.9 per cent (or 1,057,777) were domestic students and the remaining 28.1 per cent (or 413,088) were international students

In 2019, Australia's **39 comprehensive universities** employed **140,342** full-time equivalent (FTE) staff. Total FTE staff count has grown by 32.9 per cent, from 105,602 in 2008. Over the same period, the growth in academic and professional or non-academic staff was similar at around 33 per cent.

What Universities deal with

Our security perimeter is where our people are - and our people are everywhere

1. Our institutions are of national significance, yet we are culturally open
2. Research: either you are being hacked, or you are irrelevant
3. Rate of investment by criminal & nation-state attackers exceeds rate of investment by institutional defenders

The Limitations of Individual Companies in Addressing Cyber Threats

Siloed Knowledge

Companies working in isolation lack access to diverse perspectives and collective threat intelligence.

Resource Constraints

It's challenging for isolated companies to invest in the necessary security infrastructure and tools.

Lack of Scale

Individual entities may struggle to respond effectively to large-scale or coordinated cyber attacks.

Complex Regulatory Landscape

Meeting compliance requirements across multiple jurisdictions can be an overwhelming task.

Who really owns your Identity?

How can we take ownership while providing security against fraud?

Who retains the "keys" to proof/validation of who you are?

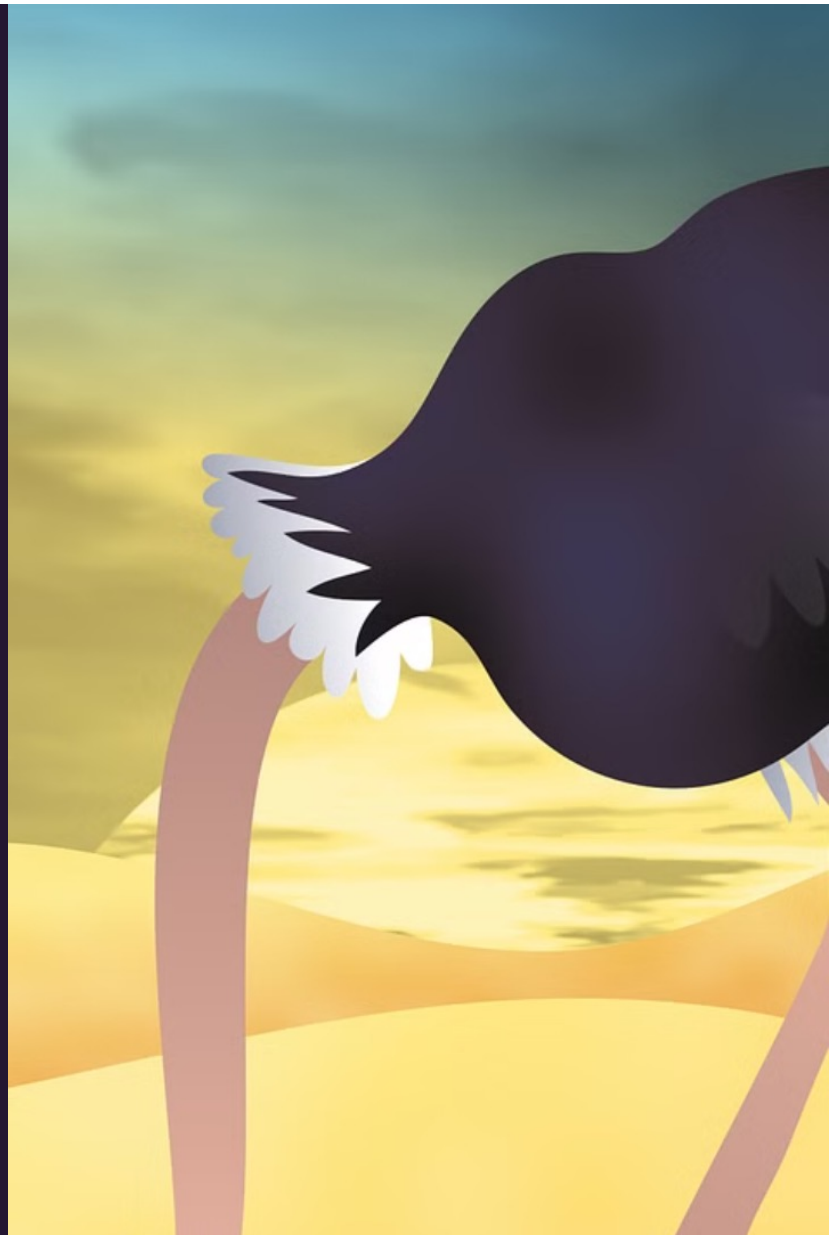
How do our systems stop creating more duplication and take advantage of other contemporary options?

Personas

1. **Staff**
   Why can't they use their own identity
2. **Students**
   Prefer to use their own identity
3. **Alumni**
   Should use their own identity
4. **Partners**
   Would have their own identity
5. **Public**
   Have their own identity

Where to from here?

1. Do we need to keep creating individual identities and their corresponding data?
2. Can we use other means to reduce friction and risk?
3. Can we rely on government to help? How can we part of the conversation?
4. Unnecessary identity and data retention is the new oil to hackers.




How we collaborate as a sector

AUSCERT

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

AUSCERT is a not-for-profit provider of cyber security services, funded entirely by membership fees.

Started and still a part of the University of Queensland.

38 universities and 4 partners participate in the AHECS Information Sharing and Analysis Centre, operated by skilled AUSCERT Cyber Security Analysts.

AUSCERT publishes 30 high confidence events

CTIS publishes 30 high confidence events

AHECS ISAC shares higher education threat information

AUSTRALASIAN HIGHER EDUCATION CYBERSECURITY SERVICE **(AHECS)**

Pioneered by CAUDIT Members - 42 Institutions

Following cybersecurity #1 Top 10 priority

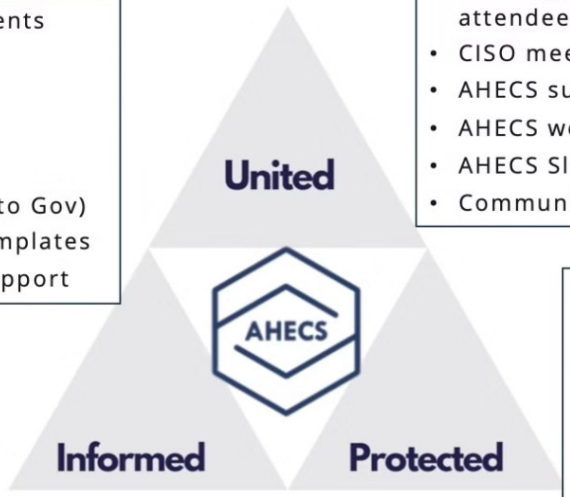
By the sector, for the sector - 500+ members

Represented by 5 partners + reps from CISO and CIO groups

“All boats lift on a rising tide”

CAUDIT cybersecurity program overview

- Third party risk assessments
- Threat intelligence
- Maturity assessments
- Leadership (AHECS)
- Advice
- Advocacy (i.e., response to Gov)
- Good practice guides, templates
- Individual operational support



- Webinars – threat briefings, case studies, training, product showcases (over 1,750 attendees to date in 2022)
- CISO meetings (monthly)
- AHECS summit
- AHECS website & online engagement
- AHECS Slack channel
- Community of practice

- Procurement offers (resource & financial savings)
- Benchmarking – baseline, systems, maturity, and employment
- Government, vendor & third-party engagement (AU, NZ, US)
- AHECS ISAC

AUSTRALASIAN HIGHER EDUCATION CYBERSECURITY SERVICE (AHECS)

AARNet

SOC by the numbers

24 Customers

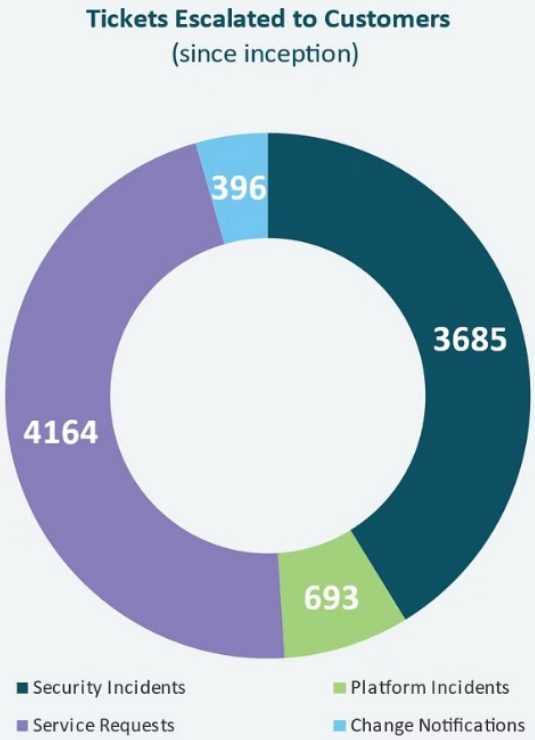
50+ Billion Logs per Day

100+ TB Average log ingestion/day

19k Unique Log Sources Onboarded

7.5k Alarms

931 Security Cases



Benefits of Industry-Based Cooperation in Cybersecurity

1

Enhanced Collective Knowledge

Pooling industry expertise enables a comprehensive understanding of emerging threats and vulnerabilities.

2

Improved Resilience

Collective defense mechanisms provide a stronger barrier against sophisticated cyber attacks.

3

Efficient Resource Allocation

Sharing resources reduces redundancy and enhances the cost-effectiveness of security measures.

4

Shared Threat Intelligence

Cyber threat information exchange is vital for preemptively addressing potential risks.

5

Interconnected Defense Systems

Integrating security frameworks leads to a more unified and interdependent protection network.

6

Collaborative Incident Response

Coordinated strategies help in timely and effective mitigation of cyber attacks across multiple entities.

Challenges and Risks of Industry-Based Cybersecurity Cooperation

Intellectual Property Concerns

Sharing sensitive data may pose risks to proprietary information and trade secrets.

Trust and Compliance

Building trust among diverse entities while complying with varying regulatory conditions is formidable.

Dependency on Others

Reliance on collaborative networks can lead to vulnerabilities if one participant is compromised.

Call to Action for Industry-Based Cybersecurity Cooperation

1

Elevated Defense Efficacy

Unifying industry forces is essential in bolstering the overall cybersecurity posture.

2

Regulatory Harmonization

Advocating for cohesive regulatory frameworks ensures streamlined cross-sector collaboration.

3

Global Collective Responsibility

Urgently addressing shared threats promotes international cyber defense synergy.

AUSTRALIA
ECU
EDITH COWAN UNIVERSITY

Creative thinkers made here.

Thank You