Impact Case Study

Enhancing Cyber Security across Australia's University Sector

Introduction and background

The continuing evolution of cyber security threats puts many elements of Australian society at risk, from individuals and businesses to government and the education sector.

To enhance the university sector's cyber security capabilities, Professor Matthew Warren, director of RMIT's Centre for Cyber Security Research and Innovation, is leading a national Cyber Security Project.

The Enhancing Cyber Security across Australia's University Sector project is an Australian Government University Foreign Interference Taskforce (UFIT) Cyber Project initiative. UFIT covers four areas relating to foreign interference: due diligence; communication and education; knowledge sharing; and Cyber Security. Refreshed UFIT Guidelines were released in November 2021.

The project commenced in June 2020. Professor Warren and his project team aim to develop a number of mechanisms that will enable a tailored, co-ordinated response to cyber threats against the University sector.

The research

UFIT is the first initiative of its kind where the university sector has been able to engage with government cross agencies to counter foreign interference.

For cyber security issues specifically, this project will complement and build on existing government and university mechanisms, such as the Cyber Threat Intelligence Sharing (CTIS) Platform integration and guidelines, to strengthen the posture of universities and government agencies when dealing with these cyber threats.

The project will develop a base for industry/university/Government partnerships to help build robust cyber capabilities in Australia's higher education sector.

The research is underway and will be completed by 30 June 2022. It will involve:

- Investigating different threat models and what is appropriate for the sector (such as MITRE, Essential 8, Information Security Manual);
- Providing recommendations to the Australian Cyber Security Centre (ACSC) on how to best integrate the university sector into the CTIS Platform;
- Identifying trends and gaps in cyber security strategies across all universities from the Tertiary Education Quality and Standards Agency (TEQSA) Annual Compacts;
- Developing sector specific, best practice Cyber Security blueprints.

Trusted forums

The project has established a series of trusted cyber security forums where relevant security issues are shared and discussed. This collaborative environment is designed to improve the sharing of cyber security intelligence and practices across the sector with senior decision-makers across university and government.

The new policy around Critical Infrastructure considers Universities to be of national significance. The forums are an avenue for an open dialogue between government and the university sector about policy changes.

Capability assessments

The project is being used to determine the University sector's current cyber security capabilities and identify critical gaps, and to advance cyber-resilience, particularly in the context of cyber security and foreign interference. The project also explores standardised mechanisms through which threat intelligence and best practice countermeasures can be shared, and common threat models developed collaboratively with participants.

What's next...

Funding support and/or institutional support

The project has received $1.6 million in funding from the Federal Government Department of Education, Skills and Employment.

Project outcomes

Cyber Security Forums & Workshops

Four trusted forums have been run to date, with the fourth taking place in November 2021. The forums have the following characteristics;

- Every University has been represented in at least one forum
- Each forum has been attended by 60-70 participants from across the sector

The audience consists of Chancellors, Vice-Chancellors, CISOs, CIOs, COOs, CROs and CFOs, as well as those in Cyber and Governance leadership roles.

The workshops' themes have included:

- Converting cyber risk into business risk
- Cyber 10 years into the future
- Using guidelines to inform cyber security strategies.

Overview of the impact

The Trusted Forums are the first shared forums between government and the university sector in relation to cyber security and foreign interference. Both speakers and audience participants have found the events valuable. Audience members have noted in their feedback on the benefits of learning more about 'the big picture' and the direct impact on businesses.

Impact on policy and practice

The project and centre are directly contributing to Australia's national Cyber Security strategy, as stated under Objective 40 of Australia's Cyber Security Strategy 2020, which says:

"Although the cyber security of the tertiary education sector is primarily the tertiary education sector's responsibility, the Australian Government is also investing $1.6 million to enhance the cyber security of Australian universities. This will fund a threat intelligence-sharing network, sector-wide threat modelling and a national cyber security forum that will meet three times a year. Strengthening the collective defences of universities against future threats will support our cyber skills agenda."

On completion, the project will have created a blueprint of best practice guidelines that are sector-specific for different sized (cyber maturity as well as location and student size) universities.

Next steps

The project is continuing till June 2022. Two Hybrid Forums – involving multiple types of engagement – will take place in March and June 2022.

The forums will take place in Canberra, with both face-to-face and virtual components. The Virtual Event platform will allow guests to participate in round tables, network, and work in groups, similar to live conferences.