

Impact Case Study

Enhancing Cyber Security

Introduction and background

Australia faces increasing cyber security threats, potentially affecting not only Australian businesses and financial institutions, but government and the education sector as well.

In response to these challenges, the Australian government established the Enhancing Cyber Security Across Australia's University Sector Project, to measure the sector's preparedness for any potential threat and to identify ways of increasing and improving the security of the sector's research, data and personnel against cyber security breaches and foreign interference.

The Enhancing Cyber Security Across Australia's University Sector Project, funded by the Department of Education, began in September 2020 and formed part of Australia's 2020 Cyber Security Strategy.

Professor Matthew Warren, Director of RMIT's Centre for Cyber Security Research and Innovation (CCSRI), was engaged to lead the research into the cyber security capability and resilience of the Australian university sector, which is considered part of Australia's critical infrastructure. The project also aimed to enhance the university sector's ability to meet evolving security threats, and to integrate its response with the broader national response to reducing and eliminating foreign interference.

Research was undertaken in consultation with the Department of Education, the Department of Home Affairs, and the Australian Cyber Security Centre.

The research

The research undertaken by the Enhancing Cyber Security Across Australia's University Sector Project was the first of its kind, in how it approached improving cyber security across the entire university sector. It built on the 2019 It the University Foreign Interference Taskforce (UFIT) Guidelines to Counter Foreign Interference.

The project's research into enhancing the Australian university sector's cyber capability and resilience involved:

- investigating the university sector's current capabilities to counter foreign interference through surveys and historical analysis;
- examining the sector's existing mechanisms to receive and share threat intelligence, and connecting the sector to existing Threat Sharing mechanism platforms;
- developing an online tool to help create further threat models and mechanisms
- developing a comprehensive suite of resources (in line with government resources) to assist universities with upskilling their entire community.

—
What's next...

Forums

Six Trusted Cyber Security Forums were held from November 2020 to June 2022, bringing together strategic leaders across government and c-suite executives in the university sector to discuss the changing cyber threat environment, establishing a community of practice.

Over 500 attendees from all 39 Australian Public Universities attended the forums, where over 30 different government, university and industry speakers presented on cyber security topics.

The research team – led by Matt Warren and including Gabby Cincotta (Senior Project Coordinator), Mary-Anne Mwendwa (Project Coordinator), and Lee-Ann Phillips (Education Designer) – ensured their research adapted to emerging cyber threats, and the changing political and legislative landscape of 2020-2022.

Funding and institutional support

The project was funded by Australia's Department of Education and is supported by the Home Affairs' University Foreign Interference Taskforce (UFIT). The RMIT Project team delivered this on behalf of all Australian Universities, for the benefit of the entire sector.

Project outcomes

The Enhancing Cyber Security Across Australia's University Sector Project research project resulted in numerous outcomes for the sector. These included 18 Project Reports as well as the following resources.

Best Practice resources

In August 2022, the project delivered a suite of best practice resources for universities to use in improving their cyber security readiness:

- 4 Handbooks;
- 5 Blueprints;
- 1 Online Tool;
- 4 Training Programs;
- 10 Supporting Training Resources (Blueprints).

Training resources

The project also developed a suite of training resources for the university sector, made of up 1.3 million students and 130,000 staff. The resources were developed to be adaptable to the different sizes and capabilities of each institution and for everyone from students to professional and academic staff and executives. The courses were validated by university representatives, who described them as:

- “some of the best I have seen in this space”;
- “this was really well-developed, at no point did I feel anything was missing”;
- “reviewed one of the course works and frankly we struggled to duplicate it”.

As of October 2022, 37 Australian public universities had been provided with access, with 35 having utilised one or multiple resources to upskill their community. The most popular resources include:

- Cyber Security for Executives Training Program
- Guidelines to Counter Foreign Interference Training Program
- Existing Cyber Security Resources Handbook
- Enhancing Cyber Security Awareness Training Program

Media releases

- <https://www.rmit.edu.au/news/media-releases-and-expert-comments>
- Enhancing the cyber security of Australia's universities | Ministers' Media Centre (dese.gov.au)
- RMIT heads up cyber taskforce for higher education sector - Training & Development - Security - iNews
- Cyber Security Project To Protect Australia Universities (cybersecurityintelligence.com)
- RMIT to lead \$1.6m uni cyber defence – Information Age

The final report will soon be made publicly available at: <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/cybersecurity>

Overview of the impact

As a result of the six Trusted Cyber Security Forums, a trusted and nationally recognised peak forum for senior university members who have accountabilities relating to cybersecurity has been established.

The RMIT Enhancing Cyber Security Project Resources also established a SharePoint site with over 40 resources made freely available to the Sector. Through the Tertiary Education Quality and Standards Agency (TEQSA), resources have been extended to the entire higher education sector.

Professor Warren presented at the 2021 Universities Australia Counter Foreign Interference Conference and at the November 2022 TEQSA Conference.

Due to the sensitivity around the issue of cyber security in the university sector, the project outputs have not been made publicly available at the request of the Department of Education, but can be made available internally if requested.

The Centre won the 2023 iNews Benchmark Award for the best educational project for the UFIT project.

Next steps

Professor Warren is currently the Chair of the TEQSA Cyber Security advisory committee. In 2023, he is in consultation with related parties to discuss the project's next steps.