Case Studies

Cybersecurity

This case study is designed to assist universities to understand how they might develop and implement cybersecurity practices in accordance with this pillar of the Guidelines to Counter Foreign Interference in the Australian University Sector. The case study is an example only. It provides a point of reference for decision makers to refer to as appropriate to their circumstances.

Protecting your research

A PhD student at an Australian university is invited to attend an overseas conference in their area of specialisation. The PhD student is asked to present on research they are conducting on new agri-business drone capabilities in partnership with a university in New Zealand. This research has been ongoing for four years and is entering its final stages of testing, with a patent being created to assist Australian and New Zealand farmers manage their large station properties.

Travel is being paid for by the conference organisers — a foreign government department — with all flights, accommodation, meals and incidentals covered for the PhD student. The student is asked to bring his presentation and present live examples of his current study, as this was of most interest to the academics and commercial attendees at the conference. This is of great interest to the PhD student and his colleagues in New Zealand as the conference is an opportunity to advertise their future product prior to release.

The student travels to the third country, bringing his university laptop, and uses a remote access card to log into his account during the presentation. During the event, the remote access information is captured by a foreign actor and a permanent access link to the university's system and to the student's research is established. Within a month of returning, the student's research has been copied and prototypes are developed, appearing on the open market. The drone technology is also adapted by the foreign country for use in military operations.

The PhD student discovers this through a contact from the conference who also had their research project copied and replicated. He immediately raises with his supervisor that his research had been compromised, prior to contacting any of the research team in the university or New Zealand partner. The supervisor escalates the issue to the CISO, and undertakes to support the student and his research.

The university has to immediately consider and prioritise the following:

- the hostile cybersecurity threat of any open links to systems
- managing communication with research teams in the university
- managing contact with the New Zealand university and their research partners
- damage to the university's reputation
- damage to the New Zealand partner university's reputation
- whether export controlled technology has departed Australia, physically or electronically, and whether Australia's export controls legislation may have been breached
- commercial loss to the universities.

The CISRO contacts the Australian Security Intelligence Organisation and the Australian Cyber Security Centre for assistance, immediately locking down their remote access service, impacting hundreds of academic staff and thousands of students. It is discovered that many network drives have been infiltrated through the unauthorised connection as the researcher had access to dozens his peers' research projects through their open network sharing practices.

The Vice-Chancellor arranges a video-conference with the New Zealand university's Vice-Chancellor and research collaborators to inform them of the security breach and outcomes. The CISO is also available to brief the New Zealand partner's security team so they can investigate for any possible breaches of their own system through shared portals in their collaboration.

The university needs to consider, review their policies and procedures relating to:

- **Communication**: Developing a communication strategy (with the New Zealand university) to inform academic staff and students why their remote access was disrupted, in addition to discussing the security breach within the sector and broader community.
- **Remote access**: Reviewing existing remote access practices and policies and how staff and students are inducted in its future use.
- **Access and travel**: Reconsidering existing security briefings and inductions for all academic staff and students relating to system access, remote access and travel, with incremental risk considerations for research staff, research teams on sensitive and critical technology, and for all those travelling for business purposes.
- **System administration**: Reviewing system administration practices for network drive sharing, collaborative research in multiple locations, and future security protocols.
- **Export controls**: Review their processes by which researchers understand the export control status of the technology they are working on and the instances where permits are required for physical exports and electronic supply of the technology beyond Australia.
- **Travel approval**: Develop a due diligence protocol for academic staff and researchers when considering business related travel, including an approval system involving the CISO and executive, which identifies and mitigates security risks if travel is supported.