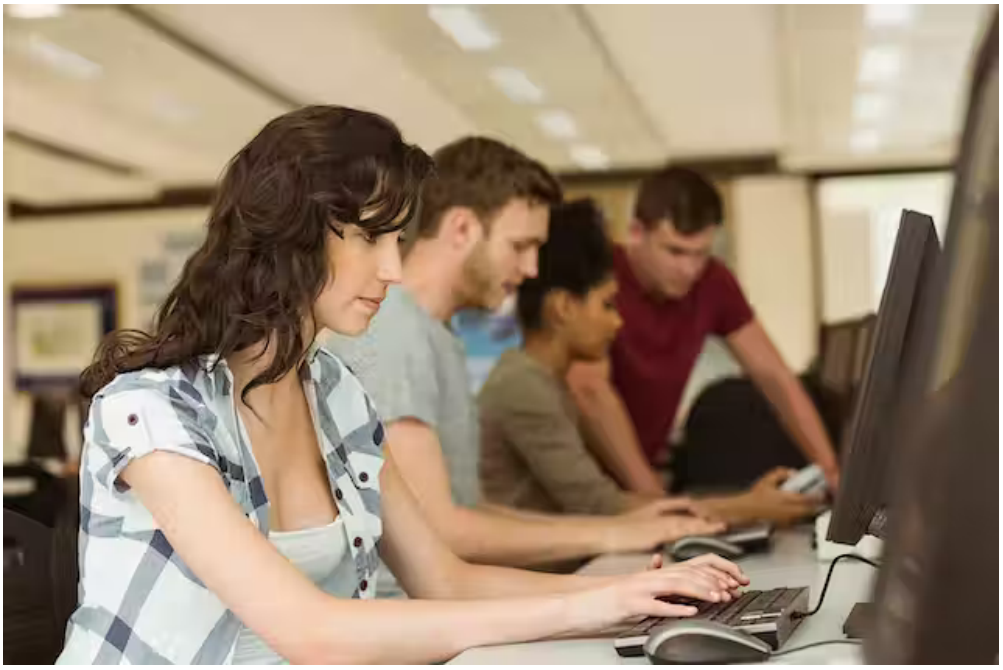
THE CONVERSATION

Academic rigour, journalistic flair



Shutterstock

Universities are a juicy prize for cyber criminals. Here are 5 ways to improve their defences

Published: September 7, 2020 9.12pm BST

Ivano Bongiovanni

Lecturer in Information Security, Governance and Leadership / Design Thinking, The University of Queensland

Karen Renaud

Visiting Professor of Cybersecurity, Rhodes University

Universities worldwide are a growing target for hackers. A July 2020 report by cybersecurity company Redscan found more than 50% of UK universities recorded a data breach in the previous 12 months.

More recently, a data breach has affected 444,000 users of ProctorU. Universities, including several Australian ones, use this online tool to supervise students sitting exams from home. Personal records from ProctorU were made available on hacker forums.

Read more: ANU will invigilate exams using remote software, and many students are unhappy

The online-first approach universities are adopting during the COVID-19 pandemic further increases their digital footprint. This was done at very short notice. This meant risk analysis was different from the traditional processes, leading to additional cybersecurity risks.

Why do unis attract attacks?

Why are universities such attractive targets? It basically boils down to higher education's "bread and butter": they hold precious data, information and knowledge. Typical examples include emails, personal information, technical resources, sensitive research data and intellectual property.

In addition, universities have attractive infrastructure – such as high-bandwidth connections via high-capacity wiring – and access to expensive resources. Their structures and processes are also inherently complex.

All of these factors make them vulnerable.

In a recently published research paper, we sought to disentangle this complexity. We interviewed 11 cybersecurity and IT leaders in universities and research centres across Australia. We asked them about the main cyber challenges their institutions faced daily.

Challenges everywhere

University IT systems host a variety of users, including academics, professional staff, students and visitors. They have different levels of knowledge and understanding of cybersecurity and could create vulnerabilities, albeit unwillingly.

At the same time, they have work to do and they sometimes feel security controls hamper their productivity. One interviewee said:

> *We regularly get pushed back by researchers saying: 'Your controls are too tight; we can't run software or do the experimentation we want to do.'*

Illustration of hacker working at laptop

Legacy systems at highly connected universities make them vulnerable to hackers. Pixabay

Universities are hyper-connected organisations, whose edges are hard to establish: the boundary is no longer simply "the campus".

Most universities also have to deal with old technology and networks. Once connected to the internet, these legacy systems may offer so-called "backdoors" that hackers can exploit. The hacking of the Australian National University and resulting data breach was an example of this.

Read more: 19 years of personal data was stolen from ANU. It could show up on the dark web

Universities increasingly operate as businesses. They connect with industry partners and third-sector organisations to make an impact on the “real world”. They outsource some of their services and develop entrepreneurial branches in the form of start-ups and spin-offs.

These activities create further complexity, as universities’ value chains are extended to involve other universities, private and public organisations and non-government organisations. A breach in one component of these value chains could have devastating effects on the other components.

Last but not least, universities have a natural inclination towards innovation. To innovate, information-sharing is essential. This, together with academic freedom, may at times clash with a culture of security. As one interviewee said:

> *The boards of directors are looking at growth, and there is no growth without risk.*

It’s all about protecting intellectual capital

Intellectual capital is the mix of human capital (the knowledge of individuals), structural capital (systems, processes and technology to organise knowledge) and relational capital (the value that comes from connections with the external world). Protecting data and information held in universities ultimately means protecting their intellectual capital.

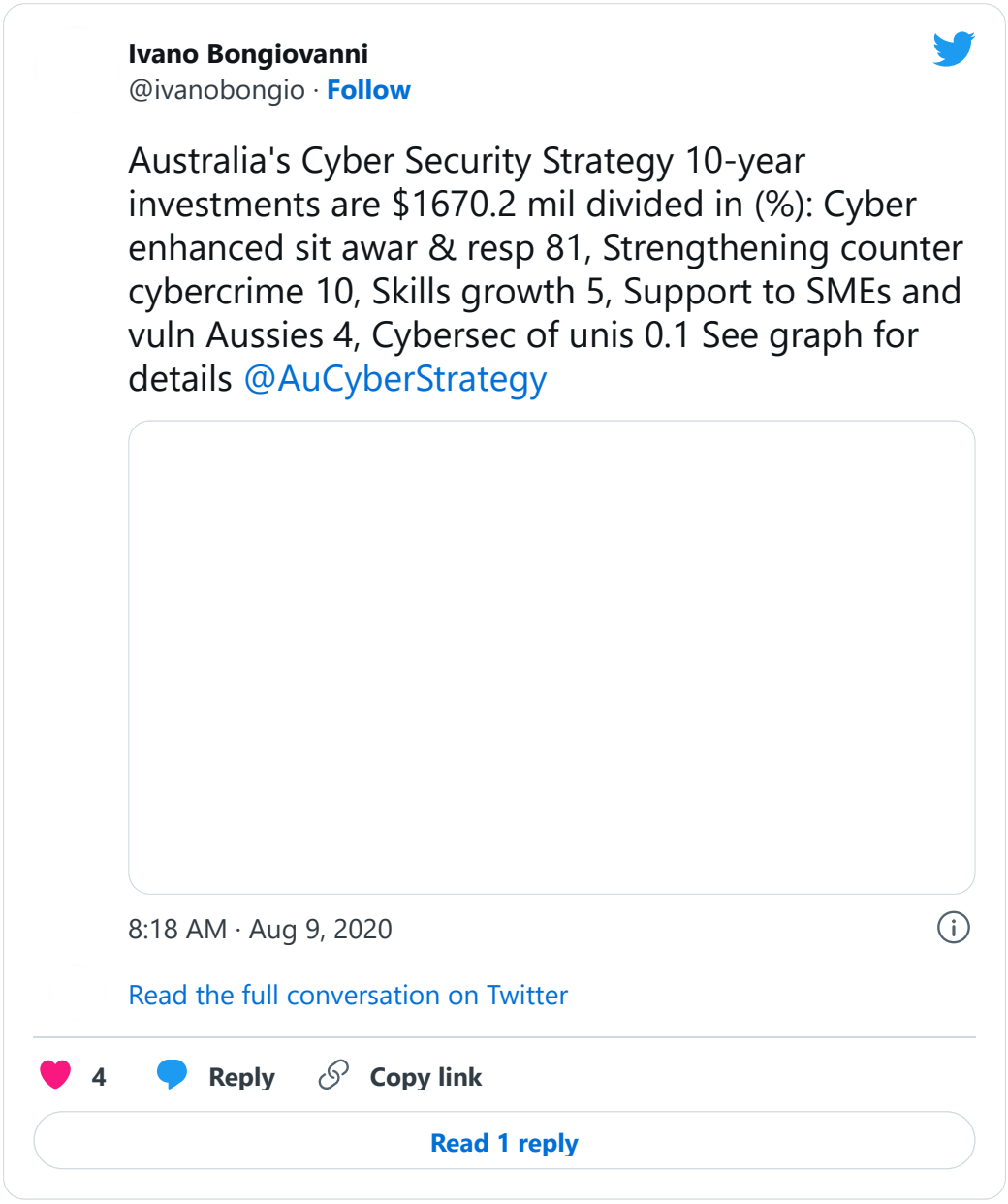
This cannot be achieved without bearing two levels of embeddedness in mind: *vertical* (the different end-user categories) and *horizontal* (the different organisations that engage with universities).

Intellectual capital protection in universities and levels of embeddedness. Author provided

Once more, this teaches us that, in cybersecurity, a one-size-fits-all approach is rarely the best solution. Even more so for universities.

Governments are acutely aware of the issues. The recently launched Australian Cyber Security Strategy dedicates A$1.6 million over ten years to enhancing the cybersecurity of universities.

Will this be enough? More money for higher education could come from critical infrastructure protection, joint cyber security centres and perhaps defence, through programs such as the Defence Industry Security Program (DISP).



Read more: Australia's cybersecurity strategy: cash for cyberpolice and training, but the cyberdevil is in the cyberdetail

What can unis do to improve cybersecurity?

Here are some suggestions:

1. Engage with all end users. Making cybersecurity easier to understand for academics, researchers, students and other users helps make them part of the solution. Engagement goes a long way towards changing people's behaviours.

2. Share information. Analysis of past breaches and chains of events – like the analysis by the Australian National University – can help other universities improve security and repel attacks. This improves cybersecurity for all.

3. Couple technology investment with investment in people. Universities such as Monash, Deakin and the University of Queensland have recently required multi-factor authentication by users. Legacy systems, where possible, should be replaced or retired, but training and awareness also have to be refined, improved and personalised.

4. Establish coalitions of universities to counter common cybersecurity challenges. This is especially important for universities that have limited resources to tackle the scourge by themselves.

5. Understand your assets. Whether holistically as intellectual capital or specifically as data, information and knowledge assets, a better understanding helps focus investments effectively and efficiently.

This article was co-authored by Dr David Stockdale, AusCERT Director and Deputy Director of Infrastructure Operations Information Technology Services at The University of Queensland.