Innovative Research Universities

Strengthening Australia's cyber security regulations and incentives: IRU response

The Innovative Research Universities supports the suite of initiatives in *Strengthening Australia's cyber security regulations and incentives*.

The IRU acknowledges that a core aim of the proposed regulatory reforms is to counter the social and economic impacts of widespread but lower sophistication threats, and notes that the Government is taking separate action to respond to sophisticated and persistent threats, including through updated critical infrastructure legislation and the University Foreign Interference Taskforce (UFIT) guidelines.

IRU considers the current, multi layered regulatory reforms approach are not easily transparent or harmonious. The discussion paper highlights universities' mixed views of the critical infrastructure Positive Security Obligations (PSO) requirements that extend to them, which are beyond the requirements applied to many other organisations.

The IRU further endorses an approach entailing broad based, fit for purpose cyber reform with applicable standards which will help clarify and strengthen universities' adherence to them. The specific requirements and actions for sectors considered of national significance under revised critical infrastructure reform should be further moderated and applied in a fit for purpose manner, subsequent to adoption of the seven new proposals under this reform.

In essence, strong, effective cyber security across all aspects of Australia is the best means to reduce the need for highly interventionist requirements under the *Security of Critical Infrastructure Act 2018* and to ensure a broad-based uplift in cyber resilience and maturity.

On this basis, the IRU is pleased to see the seven new proposals from the consultation process to strengthen general requirements and protections.

1. **Governance standards for large businesses.**

   Proposes sector-based governance standards, either co-designed as voluntary standards else implemented as mandated standards.

   It is important to ensure harmony with disparate regulatory reform and legislative amendments, and therefore the IRU welcomes Option 1: Voluntary Governance Standards in a co-designed approach as a way of broadly uplifting cyber security across the sector and minimising the disruptive impact from other reforms. This option would also be broadly complementary with the UFIT guidelines, which provide universities with key recommendations for protection.

   This and related processes are the best means to ensure effective action across the whole university system.

2. **Minimum standards for protection of personal information.**

   Proposes that a minimum code be established under the Privacy Act to increase cyber resilience through core protection-based technologies known to mitigate common vectors associated with information protection.

It is highly likely that universities already meet any such standards. The IRU endorses Option 1: Minimum standards for personal information. Universities currently apply significant efforts towards the protection standards that are mentioned in the consultation paper and to the extent there are gaps, IRU members will be keen to fill them.

The IRU also agrees that mandating ASD Essential Eight is not realistic and therefore avoiding conflict with a future code and existing best practice guidance is important. An option to achieve this is to ensure that the proposed minimum code is descriptive rather than prescriptive with the application of core technologies.

3. **Standards for security of smart devices**

Proposes introducing a new standard (adoption of ETSI EN 303 645) through legislation which would require manufacturers to implement baseline cyber security requirements for smart devices.

University students, staff and visitors are prolific users of smart devices with the internet of things use also increasing in both operations and in our research activity. It is crucial that the devices used are secure. The more secure such items are at manufacture the better for universities as major consumers, and with reduced national risk from any intrusion into university systems.

The IRU supports Option 1: Mandatory standard for smart devices and notes that while ransomware currently targets data, it is reasonable to expect that future ransomware targets are likely to include IoT, which would render physical areas inoperable and be of significant consequence for universities.

4. **Labelling for smart devices to indicate levels of security and potentially expiry date for security support.**

Proposes introducing either a Star rating-based label else a lower cost expiry label reflecting an End of Life (EoL) support timeframe for patching.

The IRU endorses Option 1: Voluntary star label. This kind of general initiative helps raise security awareness, particularly among staff and students who access university systems, as well as assists in ensuring standards for the procurement of smart devices by the sector are supported in choosing fit for purpose products.

5. **Responsible disclosure of weaknesses found in software.**

Proposes encouraging and reinforcing the current responsible disclosure of vulnerabilities as guided by the Information Security Manual and ACSC (either voluntarily, or mandatorily, through procedure).

Universities often use hundreds, and even thousands, of software systems. Responding to vulnerability reports is an essential and ongoing activity where timely response is critical. IRU members strongly support being informed in a timely fashion of any weaknesses to allow them to act in response in concert with software developers.

The IRU supports Option 1: Voluntary approaches to increasing responsible disclosure and notes that the University sector currently shares Cyber Threat Intelligence (CTI) information within a trusted community, including to an extent, information on vulnerabilities.

It is expected encouragement through procedure will increase adoption across all sectors the university engages with.

6. **Health checks for small business.**

   Proposes a cyber security health check program to provide greater support to small business.

   IRU members work with a large array of businesses. Action to encourage and assist smaller enterprises spot cyber weaknesses and address them reduces the risk that they provide an entry point into universities they work with.

   Increasingly, supply chain is used for spreading of malicious code, leading to service disruption and data breaches. The IRU supports Option 1: Cyber health checks for small business.

7. **Clear legal remedies for consumers affected by cyber incidents.**

   Proposes amendments to Australian Consumer Law to seek remedies or compensation for cyber security incidents. A direct right of action for privacy breaches is currently being explored as part of the Privacy Act Review.

   It is important for IRU members to understand fully the implications of changes to support consumers with a focus on what repercussions for incidents that originate due to attacks on university systems. The IRU members observe that cybercrime is perpetrated by criminals, and often criminals with extraordinary capability, significant resources and global reach. In efforts to support consumers, laws should not be enacted that punish the organisations that are themselves the victims of global cyber criminals.

Through effective development and implementation of the proposed suite of actions, cyber protection across Australia will be notably stronger with universities and their staff and students better protected.

These general, Australia-wide initiatives are the better way to reduce cyber incidents. They allow the Government to be highly selective and adopt a nuanced approach concerning the sectors it applies the *Security of Critical Infrastructure Act 2018* to, and the sections of that Act which it applies.

About the IRU

The IRU is a network of seven comprehensive universities committed to inclusive excellence in teaching and research in Australia. Its members are Charles Darwin University, Flinders University, Griffith University, James Cook University, La Trobe University, Murdoch University and Western Sydney University.

27 August 2021