Australian Government
Department of Education

Guidance Note

Cybersecurity

This guidance material is designed to assist universities to develop and implement cybersecurity practices in accordance with this pillar of the Guidelines to Counter Foreign Interference in the Australian University Sector. It is advisory only. It provides specific considerations for decision makers to refer to as appropriate to their circumstances.

Universities can enhance their cybersecurity posture by:

- understanding their digital assets and the relative criticality of those assets.
- implementing cyber threat modelling.
- implementing university-wide cybersecurity strategies.
- uplifting cybersecurity awareness across researchers, students and staff.
- participating in communities of practice.

Universities can also inform their approach to cybersecurity by understanding:

- The 2023-2030 Australian Cyber Security Strategy.
- The Australian Cyber Security Centre's Annual Cyber Threat Report 2023-24.

Understand and mitigate business risks proportionately

An important initial step for a university cybersecurity posture is that important digital assets are documented, and their relative criticality is well understood by risk and business owners.

Without a mature understanding of the relative importance of university digital assets, cyber security programs may lack proportionality or be more difficult or costly to implement than needed. At worst, there will be a mismatch between cyber investment and business risk resulting in critical and avoidable security gaps.

Implementing cybersecurity best practice means understanding the business risks to university operations because of cyber threats. University information systems will vary in criticality and the potential impact incurred through their loss or degradation. Due to the complexity and relative openness of university networks, particularly within research-rich environments, it is not easy to protect all assets to the same standard all at once. Universities should identify data and systems of significance to inform the priority of cybersecurity efforts. It is also likely that protective measures will need to be implemented incrementally to limit research disruption, potential impacts during exams and other critical periods, or manage project risk and cost.

Threat modelling

The formal method of linking cyber threats to risks is known as threat modelling. Once the criticality of assets if understood, threat models allow universities to map these assets to potential attack methods and various classes of threat actors (for example, state actors, criminals or insider threats)

A threat model helps to frame a cybersecurity strategy and enables university leadership to follow a risk-proportionate and sequenced set of security interventions.

Threat models may not be within reach of every university, but sharing of knowledge across universities including on available threat modelling could be valuable. Universities are encouraged to participate in communities of practice.

Threat modelling is an iterative and layered approach that links assets, vulnerabilities and threats, and aligning them to business risks to help prioritise mitigations. In general terms, a threat model will:

- define the scope for the model: whole-of-organisation or an application.
- define important assets: an asset is anything of organisational value within the model's scope, such as a specific research project or data set
- define relevant threats: threats are anything (intentional or unintentional) that may harm an organisation's assets through some technique that results in unauthorised access, destruction, disclosure modification or denial of service
- identify vulnerabilities: vulnerabilities are weaknesses that a threat actor can potentially exploit to harm the asset, such as weak passwords.

Examples of common threat models include:

- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege)
- DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability)
- PASTA (Process for Attack Simulation and Threat Analysis)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- NIST 800-151 - Guide to Data-Centric System Threat Modelling

Universities are encouraged to develop a risk-based approach, using asset criticality and threat modelling to design their cybersecurity strategies and embed these same principles and practices into solutions.

University cybersecurity strategies

Collectively, cybersecurity measures form a coherent set of organisational investments and interventions to prevent, detect, respond, and recover from cyber threats. It is not always feasible to improve all aspects of cybersecurity to the same standard at the same time. Strategic choices need to be made for areas of focused improvement, shaped by a fit-for-purpose threat model and an understanding of the business risks. Cybersecurity strategies are the mechanism by which these strategic choices are communicated to the university community.

Cybersecurity strategies help guide investment in, and the sustainment of, a group of interrelated capabilities covering people, processes, technology, and infrastructure — built around the core concept of defence-in-depth. But cybersecurity is not just about remediating current issues. A well calibrated strategy should help drive broader transformation to make sure issues do not reoccur and that universities are able to meet emergent threats. Cybersecurity strategies are not isolated from broader business change priorities such as digital transformation, and they can act as a catalyst for change beyond just security or form part of an information management framework.

Cybersecurity strategies include, but are not limited to:

- security policies, standards, guidelines, and procedures
- security roles and responsibilities
- a digital identity management component
- measures for supporting assets, vulnerability, and threat management
- key cyber security objectives and controls
- training and awareness programs
- business continuity planning and disaster recovery
- articulation of business risks arising from cyber threats.

A well developed strategy incorporates or aligns to a well understood security controls framework. While it is up to each university to choose which framework(s) best meets their needs, there are some leading practice examples that should be given strong consideration:

- The Commonwealth Information Security Manual (ISM) from which the Essential Eight and the Strategies to Mitigate Cyber Security Incidents are drawn. These are produced and published by the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) and come with a range of guidance documents.
- The US National Institute for Standards and Technology (NIST) Cyber Security Framework is a comprehensive framework with detailed information and supporting research on a broad range of controls needed to protect organisations.
- ISO 127001 provides a framework for implementing an Information Security Management System (ISMS), which is a collection of policies and processes needed to maintain the confidentiality, integrity and availability of systems and data.

Cybersecurity strategies should:

- be based on an understanding of, and be proportionate to, the threat model and business risks facing the university.
- measure the effectiveness and proportionality of the overall strategy according to the university's own relevant business continuity and information security objectives.

- incorporate metrics to assess progress against specific security objectives within the strategy and determine investment gaps.
- cover all aspects of university operations including corporate, education and research functions.
- be published along with supporting documents, such as policies and procedures, to as broad an audience as possible, and be considered for sharing across the sector.
- consider the impact of technical debt and outdated business practices which give rise to security issues.
- encompass security culture, governance, supply chain, technical controls, security skilling, and data protection.

Universities contend with legacy or dated infrastructure and large amounts of security debt, which can make options for securing such systems limited. Improving cybersecurity can also necessitate changes to underlying business practices and the replacement of costly infrastructure. These changes can be unavoidably disruptive and therefore need to be carefully planned. Cybersecurity as a whole-of-organisation "human" issue, with strong emphasis on a positive security culture.

Cybersecurity awareness

A key outcome of a cyber security awareness program should be embedding cyber-safe behaviours and decision-making across the university at every applicable level. It should promote cyber security as an enabler of academic freedom, student and staff security and emphasise its critical role in enabling the university to achieve its strategic goals.

Cyber awareness and security culture programs should consider:

- the varying challenges and expectations of different user groups, such as researchers, staff, students, visitors and executives.
- all levels of university structures, including councils, to help embed and drive a positive cyber security culture.
- being aligned to the other elements of a university's cyber security strategy.
- cyber security challenges and solutions through the lens of users, not just technology, including user-centric design principles when developing and implementing safeguards.
- the overarching principle of collective and individual responsibility in a mature cyber-safe culture.
- the promotion of cyber security capabilities as an enabler and safeguard for academic freedom and free intellectual enquiry.
- sharable approaches on creating and embedding cyber safety messages and practice mindful of the commonality of some cultural challenges, and the mobility of personnel between universities.
- measuring shifts in user behaviour and other metrics to demonstrate progress.

Communities of practice

Cyber security, while a responsibility for each individual university, has repercussions for the whole sector and for government. Our shared goals also make cybersecurity a community effort. We face similar threats, risks and common implementation challenges, and the elements of cybersecurity strategies will be comparable. Moreover, we are also producers of cyber talent and our education, research and our experience, as a community of best practice, will help ensure the sector's security and the nation's.

To strengthen this community of best practice, universities are strongly encouraged to consider actively contributing to the initiatives below. Collectively these will allow for an integrated approach to cybersecurity between universities and with Government.

- Participate in sector-wide cybersecurity forums and networks.
- Join and utilise the ACSC's threat intelligence platform: the ACSC is co-designing enhancements to its Cyber Threat Intelligence Sharing platform with government, academia, critical infrastructure, and industry partners to share threat intelligence at machine speed.
- Participate in initiatives organised by the Council of Australasian University Directors of Information Technology (CAUDIT) to help promulgate good practice, discuss common challenges and share insights into technology choices.
- Participate in sector briefings and forums convened by the ACSC and other security agencies, including making use of programs such as the ACSC partnership program.
- Consider joint incident management arrangements with other universities, to help build surge capability.
- Share insights on cyber security related technology choices.