LA TROBE UNIVERSITY | Assurance Group

Security of Critical Infrastructure Act 2018 (Cth)

FACTSHEET

Overview

The *Security of Critical Infrastructure Act 2018* (Cth) (**Act**) is the principal legislation for managing risks in relation to Australia's critical infrastructure. It allows the Australian Government to work with critical infrastructure owners and operators to identify and manage the national security risks of espionage, sabotage and coercion.

What does this mean for the University?

LTU may be a "critical education asset" under the Act if it conducts research that is critical to another critical infrastructure sector, national security or defence. If LTU does any of those things, it has mandatory notification requirements in respect to:

- critical cyber security incidents; and
- other cyber security incidents.

There may also be other information or things which LTU must provide or do if directed by the Australian Government. These will be communicated to LTU via:

- an information gathering direction;
- an action direction; and/or
- an intervention request.

A cyber security incident is one or more acts, events or circumstances involving any of the following:

(a) unauthorised access to or modification of:

i. computer data; or
ii. a computer program;

(b) unauthorised impairment of electronic communication to or from a computer;

(c) unauthorised impairment of the availability, reliability, security or operation of:

i. a computer; or
ii. computer data; or
iii. a computer program.

LTU must notify the Australian Cyber Security Centre if it becomes aware that:

(a) a cyber security incident has occurred, is occurring or is imminent; and

(b) the incident is having or has had a 'significant impact' on the availability of the critical education asset (being LTU); or

(c) the incident has had, is having or is likely to have, a 'relevant impact' on the critical education asset (being LTU)

Notification – Significant Impact

As soon as practicable, and in any event within 12 hours, after LTU becomes aware of a cyber security incident which is having or has had a significant impact, it must make a notification. This will need to be followed up within 84 hours with a written report if the initial notification was made orally.

A cyber security incident will have a significant impact if it has materially disrupted the availability of essential goods or services provided by LTU.

Notification – Relevant Impact

As soon as practicable, and in any event within 72 hours, after LTU becomes aware of a cyber security incident which is having, has had or is likely to have, a relevant impact, it must make a notification. This will need to be followed up within 48 hours with a written report if the initial notification was made orally.

A cyber security incident will have a relevant impact if it has an impact (whether direct or indirect) on the availability, integrity or reliability of the asset (being LTU) and/or on confidentiality about information relating to or stored in the asset (being LTU) or computer data.

Penalties for non-compliance

- For failing to provide a notification within a required timeframe: 50 penalty units (currently $275 per unit.
- For failing to comply with an information gathering direction or intervention request: 150 penalty units.
- For failing to comply with an action direction: 120 penalty units or 2 years imprisonment, or both.

Practical steps

Contact Andrew Morgan (Chief Information Security Officer) at andrew.morgan@latrobe.edu.au) if you:

- know or suspect a cyber security incident is occurring, is imminent or is likely to occur at LTU; or
- you identify some other sort of security risk or security issue with LTU's computer systems.

Further Information

- The Australian Cyber Security Centre homepage.
- The Australian Signals Directorate homepage.

Last updated June 2023