Module	**CYBERSECURITY**
Jurisdictions	**CTH, NSW, VIC, SA, TAS, WA, NT, QLD, ACT**
Legal Expert	**DUDLEY KNELLER** Partner at Gadens https://www.gadens.com/people/dudley-kneller/ https://au.linkedin.com/in/dudleykneller

Module application

Does your organisation have systems in place to protect its digital systems and date from a cybersecurity incident?

Does your organisation understand its obligations to manage its cybersecurity and the risks it faces from an incident?

Module scope

The CYBERSECURITY module informs the Australian organisation of their legislated legal cybersecurity obligations. The module also demonstrates effective practical advice and assistance to the organisation to implement procedures and processes that will ensure compliance and regulatory accountability throughout all levels of the Australian entity.

The CYBERSECURITY module advises the Australian organisation of the processes and procedures they need to implement to ensure compliance with all legal and regulatory obligations. Core legal and regulatory obligations are based on considerations of the broad questions determining;

- Decision making;
- Accountability;
- Stewardship;
- Direction; and
- Control

To fulfil its purpose the module focuses on providing practical assistance to the Australian organisation establishing and maintaining a robust foundational framework that determines;

- How the organisation will function;
- Who is the responsible decision maker;
- What matters are relevant to the decision-making process; and
- Whether the desired outcome has been achieved.

As entities, their employees and authorised individuals are all expected to be familiar with the broad landscape of legal obligations to which they are subject as well as more specific obligations relevant to the particular sector they are operating in, the CYBERSECURITY module should be subscribed by all Australian organisations, their employees and authorised individuals. The aim of the module is to equip the subscriber with knowledge of their obligations when operating within Australia and their obligations in New Zealand, the United States, the United Kingdom and the European Union and the circumstances in which these obligations are relevant to the Australian organisation. The module also provides the subscriber with the skills they require to establish relevant systems and processes to ensure compliance throughout their organisation.

The broad scope of the CYBERSECURITY module is to provide answers to these questions;

- What are our legal obligations?
- From where are our legal obligations derived?
- How can we ensure that we are complying with our legal obligations?
- What are the consequences if we are not complying with our legal obligations?

The CYBERSECURITY module covers all legislated legal obligations of Australian organisations and demonstrates practical assistance and guidance to ensure that these obligations are complied with through the implementation and maintenance of best practice processes throughout the organisation. The module also covers the role of the regulator as well as exemptions to the obligations, if applicable, and how they may or may not apply in particular circumstances.

The module fulfils this objective by comprehensively covering three areas;

- Legislation;
- Obligations; and
- Consequences.

1. The legislative and regulatory landscape from which the primary legal obligations are derived;

- Privacy Act 1988 (Cth);
- Protective Security Policy Framework;
- Public Service Act 1999 (Cth);
- Information Security Manual;
- Privacy Act 1993 (NZ);
- Regulation (EU) 2016/679 (General Data Protection Regulation);
- Data Protection Act 2018 (UK);
- Title 15 of the United States Code (USC);
- National Institute of Standards and Technology;
- Centre for Information Security Controls (USA);
- COBIT 5;
- Banking Act 1959 (Cth);
- Crimes Act 1914 (Cth);
- Insurance Act 1973 (Cth);
- Life Insurance Act 1995 (Cth);

- Private Health Insurance (Prudential Supervision) Act 2015 (Cth);
- Superannuation Industry (Supervision) Act 1993 (Cth);
- Prudential Standards;
- Commonwealth Risk Management Policy;
- ACSC The Essential Eight;
- Overseas acts and regulations;
- Public Sector Legislation specific to Australian states and territories; and
- Various other National and International standards and directions.

The specific areas where legal and regulatory obligations apply to the Australian organisation;

- Asset management;
  - Device and system inventory;
  - Software platform inventory;
  - Data flow mapping;
  - External systems catalogue;
  - Prioritising resources; and
  - Cybersecurity roles and responsibilities.
- Business environment;
  - Supply chain role;
  - Industry and infrastructure role;
  - Mission and objectives;
  - Critical dependencies; and
  - Resilience requirements.
- Governance;
  - Cybersecurity policy;
  - Alignment of roles and responsibilities;
  - Liabilities; and
  - Risk management processes.
- Risk assessment;
  - Asset vulnerabilities;
  - Threat intelligence sources;
  - Documenting threats;
  - Business impacts;
  - Determining risk; and
  - Identifying responses.
- Risk management strategy;
  - Processes;
  - Risk tolerance; and
  - Reviewing risk tolerance.
- Supply chain risk management;
  - Processes;
  - Risk assessment;
  - Implementation;
  - Audits; and
  - Response and recovery planning.
- Identity management, authentication and access control;
  - Authorised devices;
  - Restricting physical access;
  - Remote access;
  - Access permissions and authorisations;
  - Network integrity;
  - Identity proofing; and
  - Users and devices.
- Awareness and training;
  - User training;
  - Privileged user awareness;
  - External stakeholders;
  - Executive awareness; and
  - Security personnel awareness;
- Data security;
  - Protecting data at rest;
  - Protecting data in transit;
  - Removing, transferring and allocation of assets;
  - Maintaining capacity;
  - Preventing data leakage;
  - Verifying software, firmware and data integrity;
  - Separating network environments; and
  - Verifying hardware integrity.
- Information protection processes;
  - Baseline configuration;

- System development life cycle;
- Configuration change control;
- Data backup;
- Physical operating environments;
- Data destruction;
- Protection process improvement;
- Sharing the effectiveness of controls;
- Response and recovery;
- Testing response and recovery plans;
- Human resources practices; and
- Vulnerability management plan.

- Information systems maintenance and repair;
  - Remote maintenance;
- Protective technologies;
  - Audit event records;
  - Protecting removable media;
  - Essential capability configuration;
  - Protecting communications networks; and
  - Achieving resilience requirements.
- Anomalies and events;
  - Baseline of network operations and data flows;
  - Analysis of detected events;
  - Collection and correlation of event data;
  - Impact of events; and
  - Incident alert threshold.
- Security continuous monitoring;
  - Network monitoring;
  - Physical environment monitoring;
  - Personnel activity monitoring;
  - Detecting malicious code;
  - Detecting unauthorised mobile code;
  - External service provider monitoring;
  - Monitoring information systems configuration; and
  - Vulnerability scans.
- Detecting processes;
  - Roles and responsibilities;
  - Detection activities;
  - Testing detection processes;
  - Communication of event detection information; and
  - Continuous improvement of detection processes.
- Execution of response plan during or after an incident.
- Communication;
  - Roles and order of operations;
  - Reporting;
  - Sharing of information;
  - Co-ordination with stakeholders; and
  - Information sharing with external stakeholders.
- Mitigation of incidents;
  - Containment; and
  - Vulnerabilities
- Improve response processes by incorporating lessons learned.
- Recovery planning executed during or after a cybersecurity incident.
- Recovery communications;
  - Managing public relations;
  - Protecting reputation; and
  - Recovery activities.

Privacy and data protection legislation in Australia, New Zealand, the United Kingdom, the European Union and the United States all impose penalties for digital security breaches and failures.

Significant consequences can apply to Australian organisations, their employees and authorised individuals found to have breached or not complied with cybersecurity legal obligations. These consequences vary considerably depending on the nature and extent of the breach or failure. The *CYBERSECURITY* module covers specific consequences in detail. They can include monetary penalties, disciplinary measures and even terms of imprisonment for individuals found to have committed serious criminal offences.

The *CYBERSECURITY* module does not cover the rights or entitlements of individuals who have suffered damages or losses due to breaches of cybersecurity obligations by Australian organisations. The module does not cover the process that an entity or an individual would follow to report or seek compensation for the breach or their loss.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.