Module	**Cybersecurity**
Jurisdictions	**Singapore**
Legal Expert	**Ken Chia, Principal, Baker McKenzie. Wong & Leow**

Module Application

What are the rules under Singapore's Companies Act, Partnership Act or Limited Liability Partnership Act for a company or partnership to be incorporated in Singapore and carry out its business?

What power and authority does a company and its officers have that is granted to it in the Act and its constitutions including converting the business structure and entering into agreements?

Module Scope

The *CYBERSECURITY* module informs the Singaporean 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 Singaporean entity.

The *CYBERSECURITY* module advises the Singaporean 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 Singaporean 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 Singaporean organisations, their employees and authorised individuals. The aim of the module is to equip the subscriber with knowledge of their obligations when operating within Singapore and the circumstances in which these obligations are relevant to the Singaporean 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 Singaporean 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;
    - Companies Act 1967 (Cap. 50) (SNG);
    - Cybersecurity Act 2018 (SNG);
    - Cybersecurity (Confidential Treatment of Information) Regulations 2018 (SNG);
    - Cybersecurity (Critical Information Infrastructure) Regulations 2018 (SNG);
    - International Standards Organisation (ISO) 17799/27001;
    - Personal Data Protection Act 2012 (Cap. 26) (SNG);
    - Securities and Futures Act 2001 (Cap. 289) (SNG);
    - Overseas acts and regulations;
    - Various other National and International standards and directions.
2. The specific areas where legal and regulatory obligations apply to the Singaporean organisation;

- Critical Information Infrastructure (CII);
- Provision of information relating to potential/designated CII;
- Codes of Practice and Standards of Performance;
- Directions and appeals; and
- Cybersecurity framework and threats.
- Governance;
- Roles and responsibilities;
- Cybersecurity policy;
- Risk management framework; and
- Awareness and training.
- Cybersecurity strategies;
- Asset management;
- Cyberhygiene practices;
- Website infrastructure; and
- Identity management, access control and authentication.
- Risk management;
- E-commerce risk & fraud framework;
- Outsourcing risk framework;
- Website security risks;
- Vulnerability assessment and penetration testing;
- Work devices practices; and
- Detection processes.
- Data security;
- Safekeeping and destruction of company information;
- Data breach management plan;
- Data back up and recovery plan; and
- Data Leakage and Metadata.
- Personal data protection plan; and
- Personal data in electronic medium.
- Cybersecurity Threats / Incidents;
- Prevention measures;

- Incident response plan; and
- Communication plan.

3. Cybersecurity and Privacy and data protection legislations in Singapore imposes penalties for digital security breaches and failures.

Significant consequences can apply to Singaporean 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 Singaporean 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.