Module	**Cybersecurity**
Jurisdictions	**Hong Kong**
Legal Expert	**Carmen Tang, Partner, Hugill & Ip Solicitors**

Module Application

Does your organisation conduct business transactions or activities where interactions may create a risk of, or appear to involve, breaches of digital security or data privacy (for example, organisations that involve in e-commerce might face certain cybersecurity risks, including online fraud and credit card security)?

Is the organisation in an industry that is particularly susceptible to cybersecurity that would lead to potential cybersecurity threats (such as organisations that store a large amount of personal and confidential data, may be exposed to cyber risks of data breach and data loss)?

Module Scope

The *CYBERSECURITY* module informs the Hong Kong 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 Hong Kong entity.

The *CYBERSECURITY* module advises the Hong Kong 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 Hong Kong 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 Hong Kong organisations, their employees and authorised individuals. The aim of the module is to equip the subscriber with knowledge of their obligations when operating within Hong Kong and the circumstances in which these obligations are relevant to the Hong Kong 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 Hong Kong 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;
    - Telecommunications Ordinance (Cap. 106) (HK);
    - Crimes Ordinance (Cap. 200) (HK);
    - Copyright Ordinance (Cap. 528) (HK);
    - Electronic Transactions Ordinance (Cap. 553) (HK);
    - Trade Descriptions Ordinance (Cap. 362) (HK);
    - Personal Data (Privacy) Ordinance (Cap. 486) (HK); and
    - Personal Data (Privacy) (Amendment) Ordinance 2012 (HK).
2. The specific areas where legal and regulatory obligations apply to the Hong Kong organisation;
    - Safety of information systems and data assets;

- Data asset management; and
- Classification of data.
- Consistency in security risk assessment and audit;
- Performing security risk assessments;
- Communication and information-sharing; and
- Staff awareness training.
- Handling Information Security Incidents;
- Reporting mechanisms;
- Escalation procedure; and
- System recovery and associated stakeholders.
- Guidelines on public Wi-Fi Services;
- Controls on telecommunications and licensing; and
- Possible security threats.
- Privacy and personal data of individuals;
- Controls on direct marketing; and
- Data protection principles.
- Access to and misuse of computers in cybersecurity; and
- Distribution of obscene articles.
- Theft in cybersecurity; and
- Controls on classification of articles.
- Ecommerce and electronic transactions;
- Becoming a recognised certification authority;
- Disclosure and false information;
- Local implementation of consumer protections; and
- Global cooperation.

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

Significant consequences can apply to Hong Kong 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 Hong Kong 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.