ONC Lawyers 柯伍陳律師事務所

June 2019

Hong Kong – Cyberscurity

1. GOVERNING TEXTS

1.1 Legislation

Q: Is there a legislation (sectoral or general) specifically addressing cybersecurity? If yes, please indicate its name, its status (e.g. whether it is in force/or not) and provide a summary of its content. If more than one, please list them together with a brief description. In case there is both sectoral or general please address in separate paragraphs.

A: There is no specific legislation (sectoral or general) that addresses cybersecurity. There are legislation that deals with privacy protection and computer crimes. For example, the Personal Data (Privacy) Ordinance (Chapter ("Cap") 486 of the Laws of Hong Kong)(PDPO) deals with personal data/privacy protection and section 161 of the Crimes Ordinance (Cap.200) deals with the criminal offence of obtaining access to a computer with a criminal or dishonest intent.

1.2 Regulatory Authority

Q: Is there one or more regulatory authority? If yes, please list them together with a brief description of their role, function and powers (e.g. do they have corrective powers? Can they issue monetary fines?)

A: There is no one regulatory authority the deals with cybersecurity. Cybersecurity is dealt with by law enforcement agencies, regulators, government departments and statutory bodies.

Law Enforcement agency: The Hong Kong Police and in particular, its Cyber Security and Technology Crime Bureau deals with cyber crime matters and public education and awareness of cybersecurity.

Regulators: specific industry regulators take the monitoring initiative with respect to cybersecurity. For example, the Hong Kong Monetary Authority (HKMA), which is the regulator for the banking industry, launched the "Cybersecurity Fortification Initiative" (CFI) for the banking sector in 2016. The CFI provides a Cyber Resilience Assessment Framework for the banks to assess their own risk profiles, a Professional Development

Programme to train and certify cybersecurity professionals, and a Cyber Intelligence Sharing Platform for sharing of cyber threat intelligence among banks.

For security brokers that offer internet trading and are regulated by the Securities and Futures Commission (SFC), the SFC has a supervisory role in terms of cybersecurity over, among other entities, securities brokers by the implementation of the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading.

For personal data privacy, the regulator is the Office of the Privacy Commissioner for Personal Data that enforces the Personal Data (Privacy) Ordinance.

The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) under the statutory body of the Hong Kong Productivity Council is the centre for the coordination of computer security incident responses for SMEs and internet users.

For Government departments, cybersecurity is dealt with by the Office of the Government Chief Information Officer, which is under the Innovation and Technology Bureau of the Hong Kong Government.

1.3 Regulatory Authority Guidance

Q: Has the regulatory authority issued any guidance? If yes, please list them below with a small summary of their content.

A: HKMA – issued the Guide to Enhanced Competency Framework on Cybersecurity ("ECF-C")(December 2016) as part of the CFI for banks. The ECF-C aims to develop a sustainable talent pool of cybersecurity practitioners for the workforce demand in the banking sector and to raise and maintain the professional competence of cybersecurity practitioners in the banking industry.

In Hong Kong, under the Electronic Health Record Sharing System (EHRSS), electronic health records can be shared between public and private healthcare practitioners. The EHRSS is overseen by the Commissioner for the Electronic Health Record (eHRC). The eHRC issues polices, guidelines and procedures that cover privacy and cybersecurity on the sharing of electronic healthcare data via the EHRSS.

The SFC issued the guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading. The guidelines require all licensed or registered persons engaged in internet trading to implement 20 baseline requirements to enhance their cybersecurity resilience and to reduce and mitigate hacking risks.

2. SCOPE OF APPLICATION

Q: Please note that not all subsections will be relevant. However, please outline whether a subsection is covered under the law, by providing a definition or the definition of a concept that might be similar and discuss its application under the law.

2.1 Network and Information Systems

Under the Telecommunication Ordinance (Cap 106)(TO), sections 24 to 28 impose different criminal offences that relates to the disruption or interference of messages with respect to telecommunications services.

Telecommunications service is defined as: "*a service for the carrying of communication by means of guided or unguided electromagnetic energy or both*".

Telecommunication system means: "*any telecommunications installation, or series of installations, for the carrying of communication by means of guided or unguided electromagnetic energy or both*".

Telecommunications is defined as: "*any transmission, emission or reception of communication by means of guided or unguided electromagnetic energy or both, other than any transmission or emission intended to be received or perceived directly by the human eye*".

Section 27A of the TO aims at "hackers" and makes it a criminal offence for anyone to use a telecommunications system to knowingly cause a computer to perform any function to obtain unauthorized access to any program or data held in a computer.

2.2 Critical Information Infrastructure Operators

There is no specific law that covers this subsection

2.3 Operator of Essential Services

There is no specific law that covers this subsection

2.4 Cloud Computing Services

There is no specific law that covers this subsection

2.5 Digital Service Providers

There is no specific law that covers this subsection

2.6 Other

n/a

3. REQUIREMENTS

3.1 Security Measures

Q: Is there an obligation to have technical or organisational measures to manage risk in place? If yes, please list them.

A: There is generally no obligation to have technical or organization measures to manage risk in place but for regulated industries such as banking and licenced corporations such as securities brokers that offer internet trading, the regulators (HKMA and SFC) have issued guidelines that include the implementation of technical and organizational measures to manage and mitigate risks. Failure to comply with the Guidelines or relevant code of practice might result in disciplinary action and adverse impression on the regulated party that might affect the party's application or renewal of any licences that are issued by the regulators.

3.2 Notification of cybersecurity incidents

Q: In case of a cybersecurity incident, is there an obligation to notify the regulatory authority? If yes, please describe the process, timeline, and any other formality that needs to be adhered to. Please outline any other bodies that might be notified (in case of a cybersecurity incident, are the other subjects that need to be notified?)

A: There is no mandatory requirement to report any cybersecurity incident but if the incident involves a personal data leakage, the Privacy Commissioner advise the data users to report the matter to the regulator and also the affected victims within a reasonable time.

For regulated industries, the regulators such as HKMA and the SFC also set out in the guidelines and codes/practice manuals that the companies should report the cybersecurity incident to the regulators and customers in a timely manner.

If the company is a public listed company and the cybersecurity incident amounts to something that might materially affect the price of the listed shares if such information is disclosed to the general investing public, then under the Listing Rules that are supervised by the Hong Kong Stock Exchange, the listed company might need to make a public announcement to disclose and notify the general investing public about the cybersecurity incident.

3.3 Registration with Regulatory Authority

Q: Is registration with a regulatory authority required? If yes, please indicate which authority and the process, timeline, and any other formality that needs to be adhered to.

A: There is no general requirement for registration with a regulatory authority.

3.4 Appointment of a "Security" Officer

Q: Is there an obligation to appoint a Security Officer? If yes, please indicate its role, function and responsibilities.

A: There is no obligation to appoint a Security Officer.

3.5 Other requirements

Q: Please include any other requirement listed in the law.

A: n/a

4. PENALTIES

Q: What are the penalties in case of non-compliance? Please list both monetary and non-monetary penalties as well as their nature (criminal, civil, administrative).

A: For the offence of unauthorized access to a computer by telecommunications under section 27A of the TO, the maximum penalty is a fine of HK$25,000.

For the offence of access to a computer with a criminal or dishonest intent under section 161 of the Crimes Ordinance (Cap 200), the maximum penalty is imprisonment for 5 years.

For a cybersecurity incident that involves the disclosure of personal data of a data subject without the data user's consent with an intent to obtain a gain in money or cause loss in money, that is a breach of section 64 of the PDPO and the maximum penalty is a fine of HK$1,000,000 and to imprisonment for 5 years.

For enquiries, please contact our Litigation & Dispute Resolution Department:

E: criminal@onc.hk
W: www.onc.hk
T: (852) 2810 1212
F: (852) 2804 6311

19th Floor, Three Exchange Square, 8 Connaught Place, Central, Hong Kong