COMPUTER LAW & SECURITY REVIEW 32 (2016) 659–668

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/Information technology
Communications
Internet
Media
Law

A B S T R A C T

This column provides a country by country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

1.1. *Riding on the crest of a new wave of risks – new initiatives by the Hong Kong Monetary Authority and the Securities and Futures Commission on Cybersecurity*

Gabriela Kennedy *(Partner), Mayer Brown JSM (gabriela.kennedy@mayerbrownjsm.com);* **Karen H.F. Lee** *(Senior Associate), Mayer Brown JSM (karen.hf.lee@mayerbrownjsm.com);* ***Maggie Lee*** *(Associate), Mayer Brown JSM (maggie.lee@mayerbrownjsm.com).*

A set of initiatives in Hong Kong by the financial regulators to strengthen cyber-security requirements have taken place in the past few months. These initiatives come as no surprise given the increase in the number of data breaches and data hacks in Hong Kong in the past year alone. In fact cyber-security has been on the radar of both the Hong Kong Monetary Authority ("**HKMA**") and the Securities and Futures Commission ("**SFC**") for at least two years (see the various circulars, guidelines and other publications issued by each since 2014,[1] and the semantic shift in the language of these publications from reducing/mitigating hacking risks to clearer edicts on pre-emptive measures to increase cyber-security).

This article looks at the changes and proposals articulated in the recent initiatives of the HKMA and the SFC and their impact on financial institutions operating in Hong Kong.

1.1.1. *HKMA's Cybersecurity Fortification Initiative*

On 18 May 2016, the HKMA announced a new cybersecurity initiative unambiguously called the "Cyber-security Fortification Initiative" ("**CFI**"). The CFI is the most comprehensive cyber-security initiative developed by the HKMA to date.

The CFI applies to all financial institutions in Hong Kong supervised by the HKMA (the "**Banks**") and its aim is to enhance the cyber-security of Hong Kong's banking system through: (i) the introduction of a cyber risk assessment framework; (ii) rolling out training to ensure a steady supply of qualified cyber-security professionals; and (iii) setting up a cyber intelligence platform for Banks. The CFI will be implemented through a three pronged approach, as follows:

For further information see: www.mayerbrown.com.

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong. Tel.: +852 2843 2211.
E-mail address: gabriela.kennedy@mayerbrownjsm.com.

[1] HKMA publications: Supervisory Policy Manual module entitled "Risk Management of E-banking" dated 2 September 2015; Circular entitled "Cyber Security Risk Management" dated 15 September 2015; SFC Circulars: Circular to All Brokers – Tips on Protection of Online Trading Accounts dated 29 January 2016; Circular to All Licensed Corporations on Internet Trading – Internet Trading Self-Assessment Checklist dated 11 June 2015; Circular to Licensed Corporations – Mitigating Cybersecurity Risks dated 27 November 2014; Circular to All Licensed Corporations on Internet Trading – Information Security Management and System Adequacy dated 26 November 2014; and Circular to All Licensed Corporations on Internet Trading – Reducing Internet Hacking Risks dated 27 January 2014.

http://dx.doi.org/10.1016/j.clsr.2016.06.004
0267-3649/

1.1.1.1. Cyber Resilience Assessment Framework. The Cyber Resilience Assessment Framework is intended to establish a risk-based framework for financial institutions to self-assess their risk profiles and determine the level of security they require. The framework comprises three components:

(i) Inherent risk assessment – which measures the cyber risk exposures of a Bank based on a set of factors. Inherent risk ratings of high, medium or low will be used to set each Bank's "required maturity level" of cyber resilience.
(ii) Maturity assessment – a Bank's "actual maturity level" of cyber resilience is to be ascertained through this assessment. By comparing the actual maturity level and the required maturity level of cyber resilience, gaps in the cyber-security framework of a Bank can be identified. The HKMA will require the Bank's senior management to put in place governance arrangements and processes to achieve the required level of cyber resilience.
(iii) Intelligence-led Cyber Attack Simulation Testing ("**iCAST**") – will comprise of simulation test scenarios which are designed to replicate cyber attacks based on specific and current cyber threat intelligence. Banks which aim to attain the "intermediate" or "advanced" actual maturity levels are required to perform and satisfy an iCAST.

The inherent risk and maturity assessments should be conducted by qualified professionals who possess the necessary knowledge and expertise, such as professionals certified under the Professional Development Programme (discussed below).

The HKMA will shortly begin a three month consultation of the Cyber Resilience Assessment Framework with Banks. The details of the factors that will be considered in the inherent risk and maturity assessments and the methods of assessments will be released to Banks shortly.

1.1.1.2. Professional Development Programme. The Professional Development Programme has been devised to deal with the lack of qualified cyber-security professionals who will be needed to assist financial institutions to carry out cyber-security audits and implement adequate levels of security. The Professional Development Programme hopes to close this skills gap by boosting the supply of qualified cyber-security professionals and enhancing the sector's cyber security system.

The Professional Development Programme is a training and certification programme which has been designed jointly by the HKMA, Hong Kong Institute of Bankers ("**HKIB**") and Hong Kong Applied Science and Technology Research Institute ("**ASTRI**"). Scheduled to be rolled out by the end of 2016, the programme will provide the first set of training courses for cyber-security practitioners in Hong Kong. While initially designed for the financial sector, depending on its success it is likely other sectors might follow suit.

1.1.1.3. Cyber intelligence sharing platform. The final pillar of the CFI features a new piece of infrastructure which allows the sharing of cyber threat intelligence amongst Banks to enhance collaboration and uplift cyber resilience. The platform will be jointly launched by the HKMA, HKIB and ASTRI by the end of 2016. All Banks are expected to join the platform. This will be the first platform of its kind launched in Asia.

The platform's aim is to increase awareness amongst Banks of cyber-attacks and enable them to be prepared for attacks, by constantly sharing cyber-intelligence.

On 24 May 2016, the HKMA issued a circular[2] to all Banks mandating the implementation of the CFI. In the meantime, Banks are encouraged to actively participate in the consultation exercise for the Cyber Resilience Assessment Framework and are reminded to start making the necessary preparations to implement the CFI. The HKMA will set out further details of the regulatory requirements related to the implementation of the CFI after taking into account input from the industry during the consultation period.

1.1.2. SFC's Circular on cybersecurity

Prior to the issuance of the CFI, a Circular to All Licensed Corporations on Cybersecurity[3] (the "**Circular**") was issued by the SFC in March this year. The SFC regulates participants in the securities and futures markets which are licensed under the Securities and Futures Ordinance[4] (also known as Licensed Corporations, "**LCs**"). The Circular identified areas of concern arising out of reviews conducted by the SFC against selected LCs, including inadequate coverage of cyber-security risk assessment exercises, inadequate cyber-security risk assessment of service providers, insufficient cyber-security awareness training, inadequate cyber-security incident management arrangements and inadequate data protection programs.

In view of the outcome of the reviews, the SFC recommended cyber-security controls that could help address the weaknesses in cyber-security control frameworks and strengthen defensive mechanisms, including:

- establishing a strong governance framework for cyber-security management;
- implementing a formalised cyber-security management process for service providers;
- enhancing security architecture to guard against advanced cyber-attacks;
- formulating information protection programs to protect sensitive information flow;
- strengthening threat, intelligence and vulnerability management to pro-actively identify and remediate cyber-security vulnerabilities;
- enhancing incident and crisis management procedures with more details of latest cyber-attack scenarios;
- establishing adequate backup arrangements and a written contingency plan that incorporates the latest cyber-security landscape; and
- reinforcing user access controls to ensure access to information is only granted on a need-to-know basis.

[2] HKMA Circular entitled "*Cybersecurity Fortification Initiative*" dated 24 May 2016

[3] SFC Circular to All Licensed Corporations on Cybersecurity dated 23 March 2016

[4] Examples of LCs include market operators (e.g. exchanges and clearing houses) and intermediaries (e.g. brokers, investment advisers and fund managers).