HK's financial regulators focus attention on cyber security

In Hong Kong ('HK'), financial regulators are trying to ensure that organisations are prepared for cyber threats and are accountable for their systems, as illustrated by recent actions by the Hong Kong Monetary Authority ('HKMA') and the Securities and Futures Commission ('SFC'). Gabriela Kennedy, Karen H.F. Lee and Maggie S.Y. Lee of Mayer Brown JSM provide analysis of these initiatives and the impact on financial institutions operating in HK.

Cyber security has been on the radar of the HKMA and the 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 their language from reducing/mitigating hacking risks to clearer edicts on pre-emptive measures to increase security).

The HKMA's Cybersecurity Fortification Initiative ('CFI')

On 18 May 2016, the HKMA announced the CFI, the most comprehensive cyber security initiative developed by the HKMA to date. The CFI applies to all financial institutions in HK supervised by the HKMA (the 'Banks') and its aim is to enhance the cyber security of HK'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 three prongs:

Cyber Resilience Assessment Framework ('CRAF')

The CRAF 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 that are designed to replicate cyber attacks based on specific and current cyber threat intelligence. Banks that aim to attain the 'intermediate' or 'advanced' 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 ('PDP')(discussed below).

The HKMA will shortly begin a three month consultation on the CRAF 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.

The PDP

The PDP has been devised to deal with the lack of qualified cyber security professionals that will be needed to assist financial institutions in carrying out cyber security audits and implementing adequate levels of security. The PDP hopes to close this skills gap by boosting the supply of qualified cyber security professionals and enhancing the sector's cyber security system.

The PDP is a training and certification programme that has been designed by the HKMA, the Hong Kong Institute of Bankers ('HKIB') and the Hong Kong Applied Science and Technology Research Institute ('ASTRI'). Set to be rolled out by the end of 2016, the PDP will provide the first training courses for cyber security practitioners in HK. While initially designed for the financial sector, depending on the PDP's success it is likely other sectors might follow.

Cyber Intelligence Sharing Platform ('CISP')

This new infrastructure allows the sharing of cyber threat intelligence amongst Banks to enhance collaboration and uplift cyber resilience. It will be launched by the HKMA, HKIB and ASTRI by the end of 2016. All Banks are expected to join the CISP. Its aim is to increase awareness of cyber attacks and enable Banks 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 CRAF 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.

SFC's Circular

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 that are licensed under the Securities and Futures Ordinance[4] (Licensed Corporations, 'LCs'). The Circular identified areas of cyber security concern arising out of SFC reviews against LCs, including inadequate coverage of risk assessment exercises, inadequate risk assessment of service providers, insufficient awareness training, inadequate incident management arrangements and inadequate data protection programmes.

The SFC recommended 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 programmes to protect sensitive information flow;
- Strengthening threat, intelligence and vulnerability management to proactively identify and remediate cyber security vulnerabilities;
- Enhancing incident and crisis management procedures with more details of the latest cyber attack scenarios;
- Establishing adequate back-up arrangements and a written contingency plan that reflects the cyber security landscape; and
- Reinforcing user access controls to ensure access to information is only granted on a need-to-know basis.

It is clear that the HKMA and the SFC are urging institutions to take on a risk-based and threat-based approach to cyber security and are starting to introduce more concrete and detailed requirements to ensure Banks and LCs adopt such an approach

In short, LCs should make sure that the enhancement of their cyber security controls is being treated as a priority. LCs are required under the Circular to undertake a comprehensive and effective review and assessment of their cyber security risks, including seeking advice from third party providers/consultants if they do not possess such expertise or resources in-house, and rectify any weaknesses identified. At the same time, they are expected to comply with the cyber security standards set out in other SFC circulars on cyber security and online trading published in the last two years.

Implications

The HK regulators are paying more and more attention to enhancing cyber security. Earlier this year, the HKMA announced the establishment of its FinTech Facilitation Office to promote research on FinTech solutions, with cyber security being a key topic. More recently, the HKMA issued a further circular[5] that requires Banks to enhance their fraud management mechanisms in regards to internet banking in light of recent unauthorised share trading incidents. The SFC has expressly stated in the Circular that it intends to focus on LCs' cyber security preparedness. The regulators' emphasis has shifted from seeking system enhancement to mandating that Banks/LCs be prepared and accountable for their systems. We expect regulators to continue to issue further requirements or guidance in the near future. To maintain HK's position as a leading international financial centre, it is vital for HK's financial institutions to have in place robust cyber security and to maintain accountability for it.

Further, it is clear that the HKMA and the SFC are urging institutions to take on a risk-based and threat-based approach to cyber security and are starting to introduce more concrete and detailed requirements to ensure Banks and LCs adopt such an approach. Institutions are expected to detect their security risks and to strengthen their control frameworks accordingly. Merely complying with the minimum requirements without regard to an institution's risk profile and vulnerabilities is likely to be considered inadequate in light of the latest SFC circulars and the CFI.

Gabriela Kennedy Partner
Karen H.F. Lee Senior Associate
Maggie S.Y. Lee Associate
Mayer Brown JSM, Hong Kong
gabriela.kennedy@mayerbrownjsm.com
karen.hf.lee@mayerbrownjsm.com
maggie.lee@mayerbrownjsm.com

1. HKMA publications: Supervisory Policy Manual module Risk Management of E-banking, 2 September 2015; Circular Cyber Security Risk Management, 15 September 2015. SFC Circulars: Circular to All Brokers - Tips on Protection of Online Trading Accounts, 29 January 2016; Circular to All Licensed Corporations on Internet Trading - Internet Trading Self-Assessment Checklist, 11 June 2015; Circular to Licensed Corporations - Mitigating Cybersecurity Risks, 27 November 2014; Circular to All Licensed Corporations on Internet Trading - Information Security Management and System Adequacy, 26 November 2014; and Circular to All Licensed Corporations on Internet Trading - Reducing Internet Hacking Risks, 27 January 2014.
2. HKMA Circular, Cybersecurity Fortification Initiative, 24 May 2016.
3. SFC Circular to All Licensed Corporations on Cybersecurity, 23 March 2016.
4. LCs include market operators (e.g. exchanges) and intermediaries (e.g. fund managers).
5. HKMA Circular, Security controls related to internet banking services, 26 May 2016.