HONG KONG MONETARY AUTHORITY
香港金融管理局

Our Ref.: B1/15C
B9/29C

15 September 2015

The Chief Executive
All Authorized Institutions

Dear Sir/Madam,

Cyber Security Risk Management

I am writing to draw your attention to the growing importance of proper cyber security[1] risk management and provide some general guidance on the matter.

Although authorized institutions (AIs) should have already put in place controls and processes to manage technology risks in general, we wish to highlight that cyber security risk management still warrants AIs' special attention. It is because different cyber attacks happened or statistics published in recent years have indicated that the frequency, stealth, sophistication and the potential impact of cyber attacks are on the rise globally. Separately, cyber attacks could also be motivated by a wide range of reasons or parties, where some might aim at compromising or even damaging specific types of information/systems. Hence, different risk management measures may be needed to deal with some types of potential cyber attacks. Accordingly, there is a legitimate concern that certain conventional risk management philosophy and controls practised by AIs might need to be adjusted or enhanced to cope with the risks.

[1] Cyber security refers to the ability to protect or defend against cyber attacks. For the purpose of this circular, cyber attacks refer to attacks that target an institution's IT systems and networks with an aim to disrupt, disable, destroy or maliciously control an IT system / network, to destroy the integrity of the institution's data, or to steal information from it.

As the Board[2] and senior management of an AI have the responsibility of, among others, protecting the AI's critical assets including sensitive information of its customers, they are expected to play a proactive role in ensuring effective cyber security risk management in the AI, covering at least the following areas:

(i) Risk ownership and management accountability – Clear ownership and management accountability of the risks associated with cyber attacks and related risk management measures should be established, which should cover not only the IT function but also all relevant business lines. Since users are usually the weakest link of cyber security controls and the initial targets of cyber attacks, effective cyber security risk management entails cooperation and strong security awareness and culture[3] across a full spectrum of relevant users (including management, the staff/contractors of the AI or other offices of the banking group and relevant service providers), especially if certain cyber security controls[4] could result in inconvenience to the management or users;

(ii) Periodic evaluations and monitoring of cyber security controls – As the threats of cyber attacks are evolving in nature, the Board should request the senior management to evaluate periodically the adequacy of the AI's cyber security controls, having regard to emerging cyber threats and a credible benchmark of cyber security controls (see **Annex**) endorsed by the Board. If material gaps are identified, the Board should ensure that the senior management properly justifies and documents any acceptance of the risks arising from the gaps. More importantly, the senior management should establish a concrete implementation plan, supported by adequate staffing and financial resources, to promptly uplift the AI's cyber security controls after deciding what upgrades or alternative compensating controls are needed if the relevant risks are not accepted by the Board or senior management. In addition, the Board should also demand periodic reports from the senior management so as to monitor the overall situation and any significant risks identified out of (a) the outcome of the above evaluations and (b) the status of adherence to the AI's security policies by the IT and other relevant functions on an ongoing

---

2 For a locally-incorporated AI, the Board may delegate its oversight duties to designated Board-level committee(s). As regards the Hong Kong operations of an overseas incorporated AI, the term "Board" in this circular generally refers to the local senior management of the AI, under the scrutiny by its head office or regional headquarters.

3 As part of the AI's security awareness and culture, users at all levels should be alerted of their roles and responsibilities in defending against cyber attacks. Moreover, they should be empowered and expected to escalate to the management their concerns, if any, about poor security practices.

4 For instance, certain effective cyber security controls may restrict users' access to the Internet (e.g. unapproved websites, personal email accounts) or entail stringent controls or checking of mobile devices used by management and staff for business purposes. For users with privileged access rights to key systems, some cyber security controls may also subject them to more rigorous background checks, authentication controls or restrictions (e.g. in terms of disclosing their job-related information in social media websites or to outside parties).

basis, given that a discipline of proper security practices in all relevant functions is vital in defending against cyber attacks;

(iii) Industry collaboration and contingency planning – Since cyber attacks could aim at multiple institutions within a short period of time, the senior management should designate relevant function(s) of the AI to explore appropriate opportunities of collaborating with other institutions and/or the Police in both sharing and gathering cyber threat intelligence in a timely manner. Such intelligence sharing may help the AI and/or other institutions to get ready for possible cyber attacks. In this connection, we believe that the broader the sharing of such intelligence among AIs, the more the banking industry will be ready to address the relevant risk. To prepare for the eventualities of cyber attacks, the AI's incident response mechanism and Business Continuity Plan should also be properly enhanced (after taking into account any guidance given by all relevant authorities from time to time) and regularly tested to assure that the AI's senior management is capable of dealing with cyber attacks, even the more catastrophic ones[5], and appropriately communicating with their customers and relevant stakeholders; and

(iv) Regular independent assessment and tests – Given the highly technical nature of cyber security, it is crucial that there are sufficient cyber security expertise and resources within the responsible function(s)[6] of the AI to exercise effective and ongoing checks and balances against the above-mentioned evaluations and monitoring of cyber security controls carried out by the senior management as well as the contingency planning efforts related to cyber attacks. Such checks and balances should entail, among others, regular independent assessment and possibly penetration tests[7].

If some of the above-mentioned areas have yet to be in place in your institution, the Board and senior management of your institution are expected to strengthen their oversight in those areas so that some concrete progress (including the evaluation of your institution's cyber security controls against the benchmark as

---

[5] These may include massive destructions or corruptions of data, or simultaneous attacks to both production and backup IT systems, networks and other infrastructures, which might render conventional IT system resilience or disaster recovery arrangements ineffective.

[6] Depending on the risk governance arrangements of the AI or its banking group, the function(s) could be the AI's IT function, technology risk management function, internal audit function or similar function(s) of the banking group so long as there is a clearly defined responsibility of the function(s) to exercise checks and balances surrounding the relevant controls of the AI. Where there is a need, the AI's responsible function(s) could engage external firms with relevant expertise and resources to carry out certain work on their behalf.

[7] AIs with processes and services that are more important to the members of the public or the functioning of the financial systems of Hong Kong are generally expected to conduct periodic penetration tests having regard to their risk assessment. Please also refer to the Supervisory Policy Module (SPM) module TM-E-1 "Risk Management of E-banking" for guidance on penetration tests related to electronic banking services.

mentioned in (ii) above) should start to be evidenced in the remaining meeting(s) of the Board this year or early next year. If there is a need, the HKMA will request your institution to submit specific deliverables for us to assess the output or progress of the work.

Should you have any questions on the content of this letter, please feel free to contact Mr George Chou at 2878 1599 or Mr Tsz-Wai Chiu at 2878 1389.

Yours faithfully,

Henry Cheng
Executive Director (Banking Supervision)

Encl.

Annex

A credible benchmark of cyber security controls

At this stage, the HKMA does not prescribe what benchmark should be used by AIs' senior management to conduct periodic evaluations of the adequacy of cyber security controls. For the time being, an AI should consider its own situation when determining the benchmark that is appropriate to the institution. Apart from the guidelines or guidance issued by relevant authorities or banking industry associations[1], the AI may draw reference from international standards or sound practices (see Note below), the relevant policies adopted by the banking group as a whole, and specific cyber-related risks relevant to the business and operations of the AI. The AI should also recognize that the benchmark should be evolving in the light of technological advancements and emerging cyber threats.

In general, AIs with processes and services that are more important to the members of the public or the functioning of the financial systems of Hong Kong are expected to adopt a more stringent benchmark. For those AIs, the HKMA believes that it is prudent for their benchmark to cover, among others, the following areas of security controls although other AIs may also draw reference from the areas mentioned:

Controls that are basically preventive or detective in nature[2]*:*

(a) Registration of authorized and restriction on unauthorized devices, software and networks;
(b) Secure configuration and access controls of devices, software and networks;
(c) Identification and remediation of vulnerabilities of devices, software and networks;
(d) Controlled use of privileged user accounts of devices, software and networks;

---

[1] Including, among others, the Supervisory Policy Module (SPM) modules TM-G-1 "General Principles for Technology Risk Management", TM-G-2 "Business Continuity Planning", TM-E-1 "Risk Management of E-banking", the circular on "Customer Data Protection" issued on 14 October 2014 and the guideline issued by the Hong Kong Association of Banks on the use of Bring-Your-Own-Device.

[2] According to some industry practitioners, it is generally more cost effective for organizations to invest in the preventive and detective cyber security controls as compared with the potentially significant cost of dealing with the aftermath of cyber attacks, as illustrated in some past incidents. Moreover, individual international standards also suggest that certain controls covered under items (a) to (d) could have the most immediate impact on preventing cyber attacks.

(e) Defenses against malwares and Advanced Persistent Threats (APTs[3]);
(f) Security and access controls of application systems;
(g) Protection of customer data and sensitive information stored in, or accessible by, different media, devices, software and networks;
(h) Security related to IT systems and networks accessible by mobile devices or devices outside the AI's physical security controls;
(i) Detection of unusual activities of, and potential intrusions into, IT systems and networks;
(j) Management of security related to service providers;
(k) User education and awareness;

Controls that are mainly for dealing with contingency scenarios:

(l) Incident responses and management, including controls for digital forensic if appropriate;
(m) System resilience, including protection against distributed denial-of-services (DDoS); and
(n) Data recovery capability[4].

Note:

Although the HKMA does not currently prescribe what specific international standard(s) or sound practices document(s) should be adopted by AIs as a benchmark for evaluating their cyber security controls, the HKMA will continue to review whether a common framework should be established to benchmark the adequacy of AIs' relevant controls. In this connection, AIs may wish to refer to the following examples (some of which highlight what combinations of controls could be more cost-effective in combating cyber threats), or any other standards/sound practices documents (including national standards) that are helpful in their circumstances, for now and adopt the maturity level of controls appropriate in their own circumstances:

---

[3] There are various definitions of APTs but the term typically covers attacks in which unauthorized users gain access to systems or networks and remain there for an extended period of time without being detected. As such attacks typically involve several stages, the benchmark adopted by AIs for periodic evaluations of their cyber security controls may need to indicate the coverage of their defensive controls.

[4] To achieve a better data recovery capability, specific controls may need to be introduced or enhanced to address the risks that cyber attacks may (i) simultaneously aim at both production and backup IT systems and networks, (ii) involve massive destruction or alterations of data, or (iii) remain undetected for a long period of time, thereby increasing the risk that data in the backup medium within the retention period might have already been corrupted. Depending on AIs' own risk assessment, these may include, for instance, more frequent and offsite data backup of critical IT systems, real-time backup about changes to critical data to a separate storage location (i.e. "Continuous Data Protection", which is different from the conventional real-time offsite mirroring control), a longer data retention period, regular testing of recoverability from data backup, and more checking of data integrity in IT systems.

- *Control Objectives for Information and Related Technology (COBIT) (http://www.isaca.org/COBIT/Pages/default.aspx)*

- *SANS Top 20 Critical Security Controls (CSC) (https://www.sans.org/critical-security-controls/)*

- *Information Security Forum – Standard of Good Practice for Information Security (https://www.securityforum.org/)*

- *ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements (http://www.iso.org/iso/home.html)*

- *ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls (http://www.iso.org/iso/home.html)*

- *ISO/IEC 27035, Information technology – Security techniques – Information security incident management (http://www.iso.org/iso/home.html)*