All "Hacked" Out: The Hong Kong Securities and Futures Commission Issues Proposals to Reduce Hacking Risks

On 8 May 2017, the Hong Kong Securities and Futures Commission (SFC) issued a consultation paper inviting comments on its latest proposals ("Proposal") aimed at reducing the risks of cyber attacks in relation to Internet trading. The consultation period ends on 7 July 2017.

Plugging the Hole

Since the beginning of 2016, at least 12 licensed corporations in Hong Kong have reported 27 cybersecurity incidents, which resulted in losses to investors worth HK$110 million. In January 2017, the police informed the SFC that several securities brokers had been victims of distributed denial of service (DDoS) attacks.

Over the past few years, the SFC has issued several circulars and recommendations to licensed corporations in an attempt to reduce the continuing surge of cyber attacks and to encourage the proactive implementation of robust cybersecurity measures. Licensed corporations are encouraged not to take a back seat and be reactive when it comes to their cybersecurity. Instead, they are asked to take responsibility at a managerial level and regularly review and test their systems, and address any risks identified.

In a recent circular issued on 26 January 2017, "Alert for Cybersecurity Threats", the SFC reminded licensed corporations that they need to implement appropriate safeguards without delay in order to protect themselves against cybersecurity threats. Licensed corporations were also reminded that any material cybersecurity incidents must be promptly reported to the SFC. Other related circulars include "Cybersecurity" dated 23 March 2016 and the "Tips on Protection of Online Trading Accounts" dated 29 January 2016.

The SFC is not the only regulator that is expending time and effort to tackle cyber attacks. The Hong Kong Monetary Authority (HKMA) launched the Cybersecurity Fortification Initiative on 24 May 2016[1], which introduced a cyber risk assessment framework, rolled out training to ensure a greater pool of qualified cybersecurity professionals, and set up a cyber intelligence platform for banks.

The Proposal is the latest in a stream of efforts by financial regulators in Hong Kong to tackle the increasing risk of cyber attacks. Following a review of the cybersecurity preparedness, compliance and resilience of brokers' Internet and mobile trading systems, conducted by the SFC at the end of 2016, the SFC identified several cybersecurity measures to help reduce the risk of cyber attacks. Whilst most of these measures have already been set out by the SFC in its Code of Conduct for Persons Licensed by or Registered with the SFC ("Code of Conduct") and in previous circulars, the SFC's intention is to consolidate them into a single guideline that provides further elaboration on existing recommendations. This culminated in the issuance of the Proposal and the launch of the consultation.

The Proposal

Under the Proposal, the SFC recommends the introduction of the draft Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading ("Guidelines"). The Guidelines are divided into three different categories of requirements, which cover: (i) the protection of clients' Internet trading accounts; (ii) infrastructure security management; and (iii) cybersecurity management and supervision.

The Guidelines do not introduce any surprising requirements – they are largely consistent with the existing requirements and recommendations of the SFC to date.

---

[1] See our article entitled "Riding on the Crest of a Wave of Emerging Risks – New Initiatives on Cybersecurity by the Hong Kong Monetary Authority and the Securities and Futures Commission".

The key proposals of the SFC are as follows:

1. The SFC intends for the Guidelines to form baseline requirements that Internet brokers must comply with, and will also form an entry requirement for future Internet brokers.
2. The SFC wishes to extend the scope of application of Paragraph 18 of Schedule 7 of the Code of Conduct to cover Internet trading of securities that are not listed or traded on an exchange. Currently, Paragraph 18 of Schedule 7 of the Code of Conduct only applies to securities dealers, futures dealers, leveraged foreign exchange traders and fund managers that conduct electronic trading of securities and futures contracts that are listed or traded on an exchange. However, some Internet brokers may conduct Internet trading through systems that are not listed or traded on an exchange, and would still be subject to the same hacking risks.
3. Under the Guidelines, the SFC intends to make two-factor authentication mandatory as a security measure for logging onto customers' Internet trading accounts. Two-factor authentication involves a combination of two different types of authentication measures (e.g., a combination of a password, a hardware or software token or biometric data), and is generally accepted as an effective means to reduce the risk of hacking. The Guidelines will not state exactly what type of two-factor authentication must be implemented, and brokers will have the flexibility to choose which method they deem appropriate.
4. The proposed baseline requirements will require brokers to use a secure network infrastructure through network segmentation, to monitor and assess security patches or hotfixes issued by service providers and implement them within one month, and to promptly update anti-virus and anti-malware solutions. Measures will also need to be implemented to prevent unauthorised installation of hardware and software and unauthorised access to the system and related servers or hardware (e.g., physical security controls). Only personnel who have a need to access the internal system should be granted such access rights, and remote access should be strictly limited on a need-to-have basis. Access lists will need to be reviewed on an annual basis to ensure that they are up-to-date.
5. The SFC recognised that encrypting the brokers' entire database would cause an adverse affect on the functioning of their Internet trading systems. As such, the SFC clarified that only customer login passwords stored on the brokers' systems will need to be encrypted, as well as sensitive information (e.g., trade data) during their transmission.
6. Under the Guidelines, brokers will need to have in place robust password policies for their customers, in order to minimise any unauthorised access. For example, minimum password lengths, a requirement that passwords be changed on a regular basis, etc. Session time out controls should also be implemented. During the activation of a customer's Internet trading account or any password resets, the password should be transmitted to the customer in a secure manner to avoid interception.
7. The SFC has decided not to make it mandatory for brokers to monitor suspicious trading patterns on their customers' Internet trading accounts, and will only suggest it as an example of good practice. Due to the large volume of data being transmitted, manual and automatic monitoring would be impractical. However, the SFC still expects brokers to have in place appropriate monitoring and surveillance mechanisms that will detect any unauthorised access to a customer's Internet trading account.
8. The SFC has included customer notification requirements in the draft Guidelines, as prompt notifications concerning activities on their Internet trading accounts (e.g., notifying them when someone has logged onto their account or when a transaction has been executed, etc.) can be an effective means of identifying and stopping hackers, since customers will be alerted to any unauthorised access or transaction. Due to the large volume of trade executions that a customer may carry out, the SFC proposes to allow customers to opt out of receiving trade execution notifications (but they cannot opt out of receiving other notifications, e.g., login or password changes).

9. The SFC has emphasised the need for brokers to implement a cybersecurity risk management framework, with the board or senior management having clear ownership and accountability for cybersecurity. Responsible and executive officers who are tasked with the overall management and supervision of the brokerage Internet trading system will be responsible for establishing the cybersecurity risk management framework, including the major roles and responsibilities, with the overall accountability resting with them.
10. The Guidelines will require brokers to implement written policies and procedures setting out how a cybersecurity incident should be reported and escalated (both internally and externally, e.g., to the SFC).
11. The Guidelines will require brokers to ensure their records and documents are backed up on an off-line medium on a daily basis, and to exercise reasonable efforts to ensure that their business continuity plan and crisis management procedures deal with different potential cybersecurity incidents. However, the SFC has decided not to make it mandatory for brokers to acquire DDoS solutions despite the recent spate of DDoS attacks, in light of the cost and the effectiveness of more affordable options.
12. Under the Guidelines, brokers will need to provide annual internal cybersecurity training, which should include recent cybersecurity regulations and threats. The SFC's 2016 review revealed that, despite staff playing a crucial role in minimising cyber attacks, many brokers had never provided internal cybersecurity awareness training or had only provided it irregularly on an ad hoc basis. The Guidelines also emphasise the need for brokers to take all reasonable steps to remind customers of potential cybersecurity risks and provide recommended measures to help customers protect themselves when using the Internet trading system.
13. It is common for Internet trading systems to be provided by third party service providers, rather than being internally developed and maintained by brokers. Consistent with previous circulars issued by the SFC, the Guidelines will require brokers that outsource any activities to a third party service provider to enter into a written agreement with them that sets out the terms of service and their responsibilities. These agreements should be regularly reviewed and amended, and should provide a sufficient level of maintenance and technical support, which can be quantitatively measured (e.g., specific service levels). It is important that the services and obligations of the service provider will ensure that the brokers will be compliant with the relevant regulatory requirements. However, under the Proposal, the SFC asks those in the industry to provide feedback on whether the current service levels provided by their service provider will enable them to comply with the Guidelines, and whether they anticipate any difficulty in obtaining a higher service level from their service providers (e.g., 99.9% service uptime).

Conclusion

The review carried out by the SFC at the end of 2016 revealed that despite various cautions and guidelines in circulars issued by them so far on the subject of cybersecurity, brokers were still vulnerable to attacks. The main issues identified are: poor password policies; limited customer awareness of cybersecurity risks; inadequate monitoring and surveillance to detect unauthorised access or transactions; and insufficient resources deployed to boost cybersecurity. The draft Guidelines seek to introduce comprehensive and strict requirements and obligations on licensed corporations, the most important of which is clear ownership and accountability of cybersecurity management at the board or business management level.

Given the uptake in cloud and other outsourced services, brokers are advised to review such arrangements now in order to ensure that their service providers are willing to work with them to meet the requirements set out in the Guidelines. Many service providers may operate on standard terms and conditions, and may be reluctant to tailor their methods of operation and security measures to meet the needs of individual clients. Regardless of the expediency of the procurement of popular services, given that accountability for cybersecurity management will rest with executive officers, all existing contractual arrangements for the provision of Internet trading systems will need to be revisited.

The SFC aims to finalise the revised Code of Conduct and new Guidelines by September/October 2017. Brokers will be given a grace period of six months from the date of publication of the final Guidelines in order to implement the baseline requirements.

Contact Us

For enquiries related to this Legal Update, please contact the following persons or your usual contact at our firm.

Gabriela Kennedy
Partner
T: +852 2843 2380
E: gabriela.kennedy@mayerbrownjsm.com

Karen H. F. Lee
Senior Associate
T: +852 2843 4452
E: karen.hf.lee@mayerbrownjsm.com