SFC proposes baseline cyber security requirements for internet trading

May 2017

Hogan Lovells

SFC proposes baseline cyber security requirements for internet trading

The Hong Kong Securities and Futures Commission ("**SFC**") has issued a **paper** containing proposals to introduce cyber security guidelines under the Securities and Futures Ordinance (the "**SFO**") applicable to internet brokers (the "**Cyber Security Consultation Paper**"). Comments are open through 7 July, 2017.

Background

The Cyber Security Consultation Paper reflects a sharpening of focus by the SFC on cyber security issues. The SFC notes that in the 18 months up to 31 March 2017, 12 licenced corporations reported 27 cyber incidents – the majority involving access to clients' trading accounts. These incidents resulted in unauthorised trades to the value of HK$110 million. The Hong Kong Computer Emergency Response Team Coordination Centre is reported to have handled 6,058 cyber security incidents in 2016, an increase of 23% from 2015.

The Cyber Security Consultation Paper highlights the prevalence of a particular form of "pump and dump" scheme in which hackers gain unauthorised access to internet trading accounts and use the cash and securities in these accounts to fund the purchase of penny stocks targeted by the hackers. The hacked accounts are used to pump up the prices of these penny stocks, following which the hackers dump the stock, causing significant losses to the hacked accounts.

Against this backdrop, the SFC conducted a 2016 cyber security review which consisted of fact finding surveys, on-site inspections of brokers' technology controls, discussions with vendors to evaluate the feasibility, cost and benefits of various systems, and a benchmarking exercise against local and overseas regulations and market practices. Based on its findings, the SFC has proposed a framework of "baseline requirements" which licensed and registered persons are expected to comply with.

Existing SFC controls

Cyber security risks are currently addressed to a limited extent in the Code of Conduct for Persons Licensed by or Registered with the SFC ("**Code of Conduct**").

Paragraph 18 and Schedule 7 of the Code of Conduct contains a set of requirements for mitigating security risks which apply to electronic trading (including internet trading) of securities and futures contracts that are listed or traded on an exchange. The Cyber Security Consultation Paper proposes to extend these provisions to electronic trading of securities and futures contracts that are not listed or traded on an exchange.

The Code of Conduct requirements are stated in general terms that reflect a principles-based, "risk-based" approach, rather than imposing specific technical requirements on brokers. For example, the Code of Practice requires a licensed or registered person to ensure the trading system's "reliability, security and capacity" and have "appropriate contingency measures" in place (paragraph 18.5), and Schedule 7 of the Code of Practice requires, among other things, appropriate governance and accountability for systems, testing of systems before deployment, prompt reporting of material service interruptions, reliable authentication techniques and appropriate operating controls to prevent and detect cyber attacks.

In addition to the Code of Conduct, the SFC has over the years elaborated on a number of security and cyber risk management themes in the following circulars and publications:

- Circular on Cybersecurity (23 March 2016);
- Tips on Protection of Online Trading Accounts (29 January 2016);
- Circular on Internet Trading – Internet Trading Self-Assessment Checklist (11 June 2015);

– Circular on Mitigating Cybersecurity Risks (27 November 2014);
– Circular on Internet Trading – Information Security Management and System Adequacy (26 November 2014); and
– Circular on Internet Trading – Reducing Internet Hacking Risks (27 January 2014).

As with the Code of Conduct, the SFC's Circulars tend to be principles based rather than prescriptive in their requirements on cyber security.

That said, it is fair to say that the SFC has, however, imposed fairly limited technology risk management ("**TRM**") requirements compared to the requirements imposed by the Monetary Authority (the "**MA**") on its licensed banks, restricted licence banks and deposit-taking companies. The MA's overarching TRM principles are set out in Module TM-G-1 (General Principles for TRM) and Module TM-E-1 of the Supervisory Policy Manual (Risk Management of E-banking), and more specific guidance on the security measures expected of internet banking businesses are set out in various Circulars. As noted in our separate **alert**, the MA is currently moving forward with a Cyber Fortification Initiative that would further advance the regulation of cyber security risks in the banking industry.

The MA also regulates the outsourcing activities of authorised institutions by way of Module SA-2 of the Supervisory Policy Manual. By contrast, the SFC imposes very little control over outsourcing by market participants, although it has endorsed the internationally recognised "Principles on Outsourcing of Financial Services for Market Intermediaries" published by the International Organisation of Securities Commissions.

Proposed baseline requirements

The proposed baseline requirements are divided into three categories: (a) protection of clients' internet trading accounts; (b) infrastructure security management; and (c) cybersecurity management and supervision.

Of particular note is the requirement for two-factor authentication ("**2FA**") (i.e. requiring two forms of authentication for account access, such as a password plus a hard or virtual token). The Cyber Security Consultation Paper notes that a number of recent hacking incidents have occurred as a result of brute force attacks using applications that decode single or dual passwords, but there have been no reported hacking incidents in cases where 2FA has been enforced. 2FA has long been a requirement of the MA for internet banking systems, and the Monetary Authority of Singapore ("**MAS**") went further in December 2016 to extend this requirement to all online trading accounts with the exception of institutional investors.

The Cyber Security Consultation Paper proposes that brokers would only need to implement 2FA in respect of account logins, on the basis that the use of 2FA for placing trading orders could adversely impact the timeliness of order execution. Moreover, brokers would have discretion in deciding what type of 2FA solution is implemented as long as the solution is "commensurate with its business model".

Other noteworthy baseline requirements proposed in the Cyber Security Consultation Paper include:

– the requirement to evaluate software security patches or hotfixes released by software providers on a timely basis and, subject to evaluation, to implement them within one month from release;
– encryption of sensitive information such as client login credentials and trade data during transmission between internal networks and client devices, recognising that encryption of all data would significantly slow down

transmission which could be contrary to investors' interests;

- the requirement to conduct a review of user-access to systems on at least an annual basis;
- the need to notify clients of account activities such as system login, password reset, trade execution, third party fund transfers and changes to account information, with clients being allowed to opt-out of "trade execution" notifications only;
- the back-up of business records, client and transaction databases servers and supporting documentation in an offline medium on at least a daily basis; and
- the requirement to enter a formal service level agreement with service providers engaged for internet trading, specifying the terms of service and responsibilities of the provider, and ensuring that the services will enable the licensed or registered person to comply with the Code of Conduct and the baseline requirements. Note that this requirement is still much less prescriptive than the MA's outsourcing guidelines which specify in considerably more detail the required content of outsourcing agreements. The MA also requires notification of certain outsourcing arrangements, whereas there is no equivalent obligation for brokers.

While the proposed new measures are more prescriptive than the SFC's existing security requirements, and will go some way towards bridging the gap between the MA's and the SFC's approach to cyber security, there is still the recognition that brokers are driven by the need to remain competitive and any measures that overly compromise performance and speed would clearly be met with resistance, and could be contrary to investors' interests. The encryption of communications between brokers and clients, for example, is a challenging one, as the introduction of encryption controls will inevitably impact the speed of data transmission. By proposing to limit encryption, at this stage, to sensitive information passing between brokers and their clients and not, for example, inter-broker communications, the proposals appear to be taking a risk-based approach that address the specific problem of the "pump and dump" schemes uncovered by the SFC's research, which involved client-access passwords being compromised. More broadly, the requirements set out in the Cyber Security Consultation Paper are stated to be baseline requirements, and many of them would afford a degree of flexibility in implementation. The effect of the baseline requirements, if implemented, will be to better protect investors and also to 'level the playing field' for brokers in adopting cyber risk management measures.

Consultation period

The SFC is seeking views on the new proposals by the deadline of 7 July 2017.

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

©Hogan Lovells 2017. All rights reserved.