KPMG

Response to the SFC Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading

July 2017

Evolving regulatory requirements on electronic trading

The securities trading regulatory environment is becoming increasingly stringent, especially on cybersecurity management of electronic trading systems. The Securities and Futures Commission of Hong Kong (SFC) has released several circulars and guidelines over the past few years demonstrating the regulator's enduring recognition of the importance of cybersecurity management. On 8 May 2017, the SFC proposed a series of baseline requirements in its **Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading** to bolster the control practices of internet brokers. The Paper consolidates the control areas that SFC expects in place for internet trading systems.

27 Jan 2014	26 Nov 2014	27 Nov 2014	11 Jun 2015	29 Jan 2016	23 Mar 2016	1 Sep 2016	26 Jan 2017	8 May 2017
SFC circular on 'Reducing Internet Hacking Risks'	*SFC circular on 'Information Security Management and System Adequacy'*	*SFC circular on 'Mitigating Cybersecurity Risks'*	*SFC circular on 'Internet Trading Self-Assessment Checklist'*	*SFC circular on 'Tips on Protection of Online Trading Accounts'*	*SFC circular on 'Cybersecurity'*	*SFC Guidelines for the Regulation of Automated Trading Services*	*SFC Alert for Cybersecurity Threats*	*SFC Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading*

Key control areas the SFC expects in place

Governance and Management Oversight	Access Controls	Network Infrastructure Architecture Security	Application Controls and Processing Integrity	System Implementation, Upgrade and Modification
Vulnerability Management	Client Communication	Risk Management	Record Keeping	Vendor Management
Data Protection	Backup and Contingency	Monitoring	System Capacity	Other specific requirements

Are you prepared?

In light of the proposed baseline requirements set out by the SFC, internet brokers should review their respective cybersecurity management practices and identify any shortfall from the regulator's expectation.

Highlights of the proposed baseline requirements in the consultation paper

Control area	Proposed baseline controls	Have you considered…?
Governance and Management Oversight	Cybersecurity awareness training should be provided to all internal system users (including staff members, contractors and service providers) on an annual basis.	• Have you incorporated the latest cyber-attack scenarios into your cybersecurity awareness training programmes? • Have you included system vendors and relevant service providers as part of the audience of your cybersecurity awareness training programmes?
Access Controls	2FA is required for login by clients to their internet trading accounts.	• Have you discussed with your internet trading system vendors whether 2FA upon client login is feasible? • Have you assessed which 2FA mechanism is appropriate and most cost-effective to implement in your internet trading systems?
Data Protection	Sensitive information (such as login credentials and trade data) should be end-to-end encrypted using strong encryption algorithms during transmission between internet networks and client devices.	• Do you have a structured and effective data protection program in place to effectively identify the data flow of all sensitive information to ensure they are all protected consistently?
Backup and Contingency	Business continuity planning (BCP) and crisis management procedures should cover possible cyber-attack scenarios such as DDoS and ransomware attack.	• Have you factored all possible cyber-attack scenarios, including DDoS and ransomware, into your BCP and crisis management procedures?
Monitoring	Monitoring mechanisms should be in place to detect suspicious activity, including monitoring unusual internet protocol (IP) addresses and identifying irregular trading patterns.	• Have you been monitoring the activities in your internet trading systems? • If no, have you assessed the feasibility and impact of implementing such monitoring mechanism into the internet trading systems? • Do you have robust processes in place to handle the alerts generated from such monitoring in an efficient and effective manner?
Client Communication	Prompt notification should be sent to clients upon system login, password reset, trade execution, fund transfer to third party and changes to client and account-related information.	• Have you assessed whether automatic notification generation is feasible within your internet trading systems?

Next steps

As the Proposal is under consultation, internet brokers can start to review their controls and prepare to implement the baseline controls.

Perform a systematic review in accordance with the proposed baseline requirements and identify potential control gaps.

Consult with system vendors to evaluate the feasibility and cost of implementing the required controls in the internet trading systems.

Contact KPMG for any assistance if needed.

Contact us

Henry Shek
Partner
IT Advisory
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Alvin Li
Associate Director
IT Advisory
KPMG China
T: +852 2978 8233
E: alvin.li@kpmg.com

kpmg.com/cn