KPMG

Regulatory Updates: Insights from SFC thematic cybersecurity review of internet brokers

In light of the increasing demand on the use of internet trading platforms and emerging threats that investors and organisations are facing, the Securities and Futures Commission ("SFC") conducted a thematic review in 2019 of 55 selected internet brokers with respect to ***the Cybersecurity Guidelines ("the Guidelines")*** issued in October 2017 and ***the Code of Conduct***, to assess compliance to the relevant baseline requirements including use of Two-Factor Authentication (2FA) of licensed corporations in internet trading business in Hong Kong.

Hong Kong internet broking industry landscape at a glance

Based on the responses to the SFC's Business & Risk Management Questionnaire from August 2019 to July 2020, the following information summarised from the survey provides insights into current industry landscape:

Turnover varies for respondents but the turnover from internet trading constitutes a considerable portion for internet brokers.

Multiple internet trading platforms are made available to clients, which include desktop-based applications, mobile applications and trading websites.

Licensed firms continue to proactively allocate resources and engage third-party service providers to support internet trading applications and software.

User ID and passwords are adopted as "what a client knows" and different methods have been used by respondents as "what a client has" as a second factor for authentication by internet trading service providers.

With the adoption of 2FA solutions and implementation of the Guidelines, there are no reported incidents of hacking of client accounts from 2016 to 2019.

How to enhance your security controls around clients' internet trading accounts

The following tables outline observations derived from the thematic review of selected internet brokers and suggest good practices that would help licensed organisations ensure compliance with the baseline requirements set in the Guidelines, as well as to provide further guidance on enhancements of current security controls.

Domain | Deficiencies and Instances of Non-compliance | Baseline Requirements | Good Practice Adopted by Inspected Firms

Protecting Clients' Internet Trading accounts

2FA

- ☒ Use of Email OTP as second authentication factor
- ☒ Deactivation of 2FA for system login
- ☒ Device binding or registration:
  - Existence of security loopholes
  - Unlimited number of bound devices allowed
  - Concurrent logins for registered devices

- ☑ Deliver OTPs through secure means including SMS, hardware tokens, and device bound to the firm's internet trading system
- ☑ Enforce the use of 2FA and prohibit clients from deactivating the 2FA function
- ☑ Internet brokers should:
  - Perform regular technical assessments to identify security loopholes
  - Only allow clients to bind a limited number of devices
  - Implement controls over concurrent logins

Implementing Monitoring and Surveillance Mechanisms

- ☒ Manual reviews alone cannot effectively identify suspicious unauthorised transactions
- ☒ Monitoring and surveillance are performed on a monthly, quarterly or ad-hoc basis
- ☒ Identical generic IP addresses mistakenly assigned to all login attempts for users

- ☑ Implement effective monitoring and surveillance mechanisms based on the account scale and trading volumes of trading operations
- ☑ Perform monitoring and surveillance at least on a daily basis;Identical generic IP addresses mistakenly assigned to all login attempts for users
- ☑ Conduct sufficient technical and user testing before implementing automated IP address monitoring tools

- ☑ Implement computer-assisted monitoring tools
- ☑ Implement Intrusion Detection System (IDS) to monitor network and systems

Prompt Notification to Clients

- ☒ Notifications not provided after certain actions (e.g. password reset)
- ☒ Opt-out of receiving notification for password reset is allowed

- ☑ Notify clients promptly after specified client activities
- ☑ Prohibit clients from opt-out of notifications other than either "trade execution" or "system login"

Data Encryption

- ☒ Weak encryption algorithms used for internet trading systems *(e.g. SSL 3.0; TLS 1.1 and below; 3DES MD5; RSA1024; SHA-1)*

- ☑ Adopt encryption algorithms that meet international security standards *(e.g. TLS 1.2 and above; AES; ECC)*

- ☑ Use of salting in the hashing algorithm

Protecting Client Login

- ☒ Client login passwords are neither randomly generated nor required to be changed upon first login to the trading system

- ☑ Ensure client login passwords are delivered in a secure manner (i.e. *either* randomly generated or adequate compensating security controls are implemented) for account activation and password reset

Stringent password policies and session timeout controls

- ☒ Password policies fail to meet baseline requirements
- ☒ Session timeout not enforced
- ☒ Deactivation of session timeout due to technical error

- ☑ Set up stringent password policies that meet the baseline requirements
- ☑ Enforce session time-out with proper idle timeout period
- ☑ Perform sufficient testing to ensure controls are properly configured

Infrastructure Security Management

Deploying A Secure Network Infrastructure

- ☒ System servers and databases reside within a DMZ
- ☑ Protect critical systems with proper network segmentations
- ☑ Place internet trading applications and critical systems within the internal network behind a DMZ
- ☑ Host servers with less sensitive data
- ☑ Deployment of multi-tiered firewall
- ☑ Implementation of anti-DDoS
- ☑ Implementation of anti-APT and web application firewall

User Access Management

- ☒ Inadequate access granting procedures and excessive rights granted
- ☑ Implement proper access control procedures and conduct user access reviews at least annually
- ☑ Implementation of PIM or PAM solution
- ☑ Deployment of automated user access recertification

Security Controls for Remote Connections

- ☒ Permanent remote access granted to vendor
- ☑ Grant temporary access to external parties on a necessity basis with a reasonable time frame (e.g. 3 to 6 months) or regularly review the access rights
- ☑ Implementation of MFA for remote access
- ☑ Use of VPN for remote connections

Patch Management

- ☒ Security patches not evaluated, tested and implemented in time
- ☒ Use of End-of-Life (EOL) software
- ☑ Evaluate, test, and deploy security patches in a timely manner
- ☑ Monitor the validity of software and replace or upgrade EOL software

System and Data Backup

- ☒ Sufficient backup not performed for business records, supporting database and facilities
- ☑ Conduct backup for business records, supporting database and facilities at least on a daily basis
- ☑ Adopt proper recovery method
- ☑ Perform restoration tests of backups at least annually

Contingency Planning for Cybersecurity Scenarios

- ☒ Cybersecurity scenarios not covered in contingency plans
- ☑ Include cyber-attack scenarios in the contingency plan and crisis management procedures

Cybersecurity Management and Supervision

R&R of Cybersecurity Management

- ☒ Insufficient assignment of Roles and Responsibilities (R&R) for cybersecurity risk management
- ☒ Insufficient IT audits or self-assessments performed
- ☑ Clearly define a cybersecurity risk management framework and corresponding Roles & Responsibilities
- ☑ Review compliance with the baseline requirements at least on an annual basis.
- ☑ Perform penetration testing
- ☑ Insurance coverage for cybersecurity incidents
- ☑ Establish SOC
- ☑ Perform gap analysis with global and regional requirements

Cybersecurity Incident Reporting

- ☒ Insufficient escalating and reporting procedures for cybersecurity incidents
- ☑ Establish written policies and procedures on escalating and reporting of cybersecurity incidents to internal and external parties
- ☑ Formulate notification and suspension processes for identified client accounts with unauthorised access.

Cybersecurity Awareness Training for Internal System Users

- ☒ Insufficient cybersecurity awareness training provided
- ☑ Provide cybersecurity awareness training to all internal users at least annually
- ☑ Subscribe to threat intelligence services

How to Ensure Compliance with Code of Conduct Requirements for Mobile Trading Applications

Cybersecurity Management and Supervision

Detective Control

- ☒ Lack of control to detect and block compromised devices
- ☑ Implement controls to detect and block compromised devices

Source Code

- ☒ Lack of control to prevent source code from being found and easily understood, which allows hackers to repackage and bypass security controls
- ☑ Obfuscate source codes to prevent potential manipulation

Sensitive Information Stored on User's Devices

- ☒ Caches of stored sensitive information allowed for mobile trading applications
- ☑ Purge client's sensitive information from mobile trading applications once clients exit or log off from the applications

Biometric Authentication

- ☒ Biometric authentication not disabled after many failed attempts
- ☒ Biometric authentication allowed after facial images or fingerprints have been updated in mobile devices
- ☑ Tighten security controls to avoid abuse of biometric authentication function

How KPMG Can Help

In response to strengthening baseline requirements, firms that provide internet trading services should take actions to review security controls in place and comply with regulatory requirements and industry standards. Our dedicated cybersecurity team is able to assist you on:

Assess your current security controls and perform gap analysis against regulatory baseline requirements and industry good practices.

Conduct professional security testing for systems and applications to uncover technical vulnerabilities that could pose a threat to systems and organisations.

Develop improvement plans to enhance your current security mechanisms and evaluate the feasibility of implementing technical controls.

Support you in overall project management for implementation of improvement plans and technical controls.

Support you in developing a robust cybersecurity governance structure and processes around management oversight.

Design security awareness training programmes to improve the overall security awareness around cybersecurity risks.

Contact us

Henry Shek
Partner, Technology Consulting,
KPMG China
T: +852 2143 8799
E: henry.shek@kpmg.com

Brian Cheung
Director, Technology Consulting,
KPMG China
T: +852 2847 5026
E: brian.cheung@kpmg.com

John Chiu
Associate Director, Technology Consulting,
KPMG China
T: +852 2847 5096
E: john.chiu@kpmg.com

Kenneth Kwan
Associate Director, Technology Consulting,
KPMG China
T: +852 2685 7390
E: kenneth.kwan@kpmg.com

kpmg.com/cn