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.

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

<table>
<thead>
<tr>
<th>Control area</th>
<th>Proposed baseline controls</th>
<th>Have you considered…?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and Management</td>
<td>Cybersecurity awareness training should be provided to all internal system users (including staff members, contractors and service providers) on an annual basis.</td>
<td>• 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?</td>
</tr>
<tr>
<td>Oversight</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Controls</td>
<td>2FA is required for login by clients to their internet trading accounts.</td>
<td>• 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?</td>
</tr>
<tr>
<td>Data Protection</td>
<td>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.</td>
<td>• 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?</td>
</tr>
<tr>
<td>Backup and Contingency</td>
<td>Business continuity planning (BCP) and crisis management procedures should cover possible cyber-attack scenarios such as DDoS and ransomware attack.</td>
<td>• Have you factored all possible cyber-attack scenarios, including DDoS and ransomware, into your BCP and crisis management procedures?</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Monitoring mechanisms should be in place to detect suspicious activity, including monitoring unusual internet protocol (IP) addresses and identifying irregular trading patterns.</td>
<td>• 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?</td>
</tr>
<tr>
<td>Client Communication</td>
<td>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.</td>
<td>• Have you assessed whether automatic notification generation is feasible within your internet trading systems?</td>
</tr>
</tbody>
</table>

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG, a Hong Kong partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.