

15 September 2023

Circular to intermediaries

Cybersecurity review of selected licensed corporations

The Securities and Futures Commission (SFC) will commence a cybersecurity review of selected licensed corporations (LCs) with a focus on assessing their cybersecurity management and compliance as well as the resilience of their information systems against cybersecurity threats.

Cybersecurity is a major focus of the SFC's supervision of LCs. All LCs should comply with the system security-related requirements stipulated in the Code of Conduct¹, amongst other requirements. LCs which offer internet trading are also required to comply with the baseline requirements set out in the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Cybersecurity Guidelines), the cybersecurity frequently asked questions² (FAQs) and the expected standards set out in the Report on the 2019-20 thematic cybersecurity review of internet brokers³.

In general, the SFC has noted that LCs have implemented some security controls to protect clients' internet trading accounts. Nevertheless, some firms are not vigilant about cyber risks and may not have sufficient control measures in place to defend their information systems and data.

The cybersecurity incidents reported to the SFC by some LCs in recent years and the SFC's inspection findings show a number of security loopholes and deficiencies, including the use of end-of-life⁴ software as well as inadequate controls over remote access and phishing attacks which hackers may easily exploit to infiltrate LCs' information systems.

Additional cyber risks may arise from advances in technology. The SFC has noted that many LCs employ third-party technology vendors to supply and support business application systems⁵ and their underlying network infrastructure, and an increasing number of firms host their systems and data in the cloud environment.

To better assess the industry's preparedness for and resilience to cyber risks, the SFC will commence a cybersecurity review in September 2023. As part of this review:

- a) the SFC will conduct a survey of selected LCs of different sizes and business types, including securities and futures brokers, leveraged foreign exchange traders, global financial institutions and firms which provide online product distribution platforms. The survey will generally cover:

¹ Paragraphs 4.3 and 18.5 of and paragraph 1.2 of Schedule 7 to the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission.

² The Cybersecurity Guidelines and the Cybersecurity FAQs were issued by the SFC in October 2017.

³ The report was issued by the SFC in September 2020.

⁴ This refers to software which has reached the end of its useful life and its vendor has stopped supporting it (eg, Windows Server 2008). Hence, the latest security patches and fixes cannot be applied.

⁵ Examples include electronic trading systems and back-office settlement and accounting systems.

- (i) cybersecurity management and incident reporting;
 - (ii) cybersecurity controls to ensure the confidentiality, integrity and availability of systems and data;
 - (iii) cloud security controls and governance;
 - (iv) remote access controls;
 - (v) lifecycle management for information technology assets; and
 - (vi) the management of cybersecurity risks from systems outsourced to third-party technology vendors;
- b) the SFC will meet with selected LCs to better understand their cybersecurity governance and controls; and
- c) the SFC will perform on-site inspections of some of the selected LCs for a deep dive review of their information technology and related management controls and an assessment of their compliance with the Cybersecurity Guidelines and other expected standards.

The findings of the cybersecurity review would form the basis for the SFC to issue further guidance to the industry. Where appropriate, the SFC will also share the observations and findings of the cybersecurity review with the industry.

Should you have any queries regarding this circular, please contact Ms Kammy Kwok on 2231 1455.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

SFO/IS/021/2023