

6 February 2025

Circular to licensed corporations

Cybersecurity review of licensed corporations

The Securities and Futures Commission (SFC) today issued its [Report on the 2023/24 Thematic Cybersecurity Review of Licensed Corporations](#) (Report), to highlight the key observations from its cybersecurity review.

The Report is based on the SFC's recent thematic review of selected internet brokers'¹ compliance with the Cybersecurity Guidelines² and Code of Conduct³ (collectively referred to as "Cybersecurity Requirements") and the cybersecurity incidents reported by licensed corporations (LCs) in the past years. The Report sets out expected standards in relation to phishing detection and prevention, use of end-of-life⁴ (EOL) software, remote access and third-party IT service provider (Third Party Provider) management and cloud security.

Cybersecurity incidents

LCs reported eight material cybersecurity incidents between 2021 and 2024. Some of these had caused significant business disruptions or hacking of client accounts. Specifically, it was noted that:

- in two cases, the LCs suffered ransomware attacks (potentially instigated by hackers through phishing) that impacted all their IT systems, including internet trading systems, settlement and back-office systems, causing severe disruption to business operations;
- in another case, one LC reported an incident where its back-office services were disrupted when its vendor's network was compromised and it did not have adequate contingency plan in place; and
- some of these incidents involved security loopholes in the LC's network, through which fraudsters gained access to the LC's trading systems and made unauthorised changes to client data. The fraudsters then gained control of the victim clients' account and conducted unauthorised transactions.

In addition, in some cases, the LCs concerned used EOL software in their systems and servers, which may have contributed to these cyber-attacks.

LCs are reminded to be vigilant about potential cybersecurity threats, identify and rectify the vulnerabilities in their networks and systems and take proactive actions to protect themselves and their clients from cyber-attacks.

¹ Internet brokers refer to licensed corporations which are engaged in internet trading and are licensed for (i) Type 1 regulated activity (dealing in securities); (ii) Type 2 regulated activity (dealing in futures contracts); (iii) Type 3 regulated activity (leveraged foreign exchange trading); and/or (iv) Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities.

² Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Cybersecurity Guidelines).

³ These include paragraphs 18.4 to 18.7 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct) and paragraphs 1.1, 1.2.2 to 1.2.8, 1.3 and 2.1 of Schedule 7 to the Code of Conduct.

⁴ EOL software refers to software which has reached the end of its useful life. The software provider has stopped supporting it and no updated security patches and fixes are available.

Compliance with the Cybersecurity Requirements

Compared to the same review in 2020⁵, we noted an improvement in compliance with some of the cybersecurity requirements and expected standards, including mobile security. However, we still noted deficiencies in certain critical areas, which may expose internet brokers to significant cybersecurity risks. For example, unqualified two-factor authentication is used for system login, lax security control configurations of the system servers and firewall⁶, delay in implementing security patches and hotfixes released by software providers, weak algorithm used for encryption of sensitive data and inadequate encryption for data-in-transit and data-at-rest, and excessive user access to system admin accounts of critical systems and databases.

Furthermore, in some cybersecurity incidents, it was noted that there was a lack of audit trail in the key systems and servers. This hindered the LCs' ability to conduct regular monitoring and investigations upon the occurrence of cybersecurity incidents.

In this connection, LCs are reminded to implement adequate cybersecurity controls to protect their systems, client accounts and data. LCs should pay particular attention to, amongst other things, the following areas:

- (a) *Network security*: LCs should implement appropriate controls to prevent and detect unauthorised intrusion, security breach and security attack⁷. LCs should, amongst other things, disable all unnecessary service ports in their servers, review and revise (where applicable) their network access control list and ensure that access to their networks are granted on a need-to-have basis.

LCs, particularly large internet brokers, are strongly advised to conduct a comprehensive technical cybersecurity review, which includes, amongst other things, vulnerability scanning, system server and workstation security hardening control review and network and application penetration testing, on a regular basis (at least annually). The review results, rectification plan and remedial actions taken should be reviewed and endorsed by the Manager-In-Charge (MIC) of Overall Management Oversight (OMO) and MIC of Information Technology (MIC-IT).

- (b) *Patch management*: LCs should monitor the security patches or hotfixes released by software providers and, subject to evaluation, conduct testing as soon as practicable and implement the security patches or hotfixes within one month following the completion of testing⁸.
- (c) *Data encryption*: LCs should apply a strong encryption algorithm to encrypt sensitive information, including client particulars (such as telephone number and email address) and user credentials. For the avoidance of doubt, both data-in-transit (including data

⁵ For details, please refer to the Circular to licensed corporations – Review of internet trading cybersecurity dated 23 September 2020 (2020 Cybersecurity Review Circular).

⁶ For example, unnecessary service ports of system servers, such as File Transfer Protocol and Secure Shell, were opened, and unnecessary access was allowed in the access control list of the firewall.

⁷ Paragraph 1.2.4(c) of Schedule 7 to the Code of Conduct.

⁸ Paragraph 2.4 of the Cybersecurity Guidelines and paragraphs G(i) and G(ii) of the 2020 Cybersecurity Review Circular.

transmitted within the internal network of LCs) and the data-at-rest should be encrypted⁹.

- (d) *User access rights*: LCs should ensure that system access rights are granted on a need-to-have basis¹⁰. In particular, users should be given the minimum number of functions necessary to enable them to perform their day-to-day duties. In addition, the system admin accounts to critical systems and databases should only be granted to a limited number of users and the usage of these accounts should be logged and monitored.
- (e) *Audit logs*: LCs should retain and review the logs for the activities in all critical servers¹¹, network devices and databases to identify and follow-up on any suspicious unauthorised activities¹².
- (f) *Monitoring of client accounts*: LCs should implement an effective monitoring and surveillance mechanism to detect unauthorised access to clients' internet trading accounts¹³. In addition to monitoring the IP address for accessing the client accounts¹⁴, LCs should regularly review changes made to client particulars in the systems and database and promptly identify red flags associated with unauthorised changes to client particulars¹⁵ for follow up actions, where required. For example, multiple clients changed their mobile phone number to the same phone number, large number of changes requested by clients using the same or similar IP address or within a short period of time and manual changes made by staff directly in the system.

Emerging cybersecurity threats and risks

As mentioned above, the LCs involved in some cybersecurity incidents used EOL operating systems¹⁶ and unpatched virtual private network (VPN)¹⁷ solutions. Additionally, some of these incidents also involved ransomware attacks, which were potentially initiated by hackers through phishing.

Given the trends of digitalisation and automation, it has become more common for LCs to engage Third Party Providers to provide IT services to support their businesses. Their services include application development and maintenance service, IT operation support service, infrastructure and network service, as well as system and data hosting service. While leveraging these providers' technology and services can be beneficial, potential cybersecurity breaches by the providers could lead to system disruption, data leakage and

⁹ Paragraph 1.4 of the Cybersecurity Guidelines.

¹⁰ Paragraph 2.2 of the Cybersecurity Guidelines, paragraph 20 of the Appendix to the Management, Supervision and Internal Control Management Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission (Internal Control Guidelines) and paragraphs 11 and 12 of the Suggested Control Techniques and Procedures for Enhancing a Firm's Ability to Comply with the Securities and Futures (Client Securities) Rules and the Securities and Futures (Client Money) Rules.

¹¹ If LCs use email to support essential business operations, such as sending payment instruction, the email server is considered to be a critical server. As such, LCs should ensure that all activities in the email servers are properly logged, retained and reviewed.

¹² Paragraph IV(6) of the Internal Control Guidelines.

¹³ Paragraph 1.2 of the Cybersecurity Guidelines.

¹⁴ Answer to question 3 of the Frequently Asked Questions on Cybersecurity issued on 27 October 2017.

¹⁵ Paragraph 1.2 of the Cybersecurity Guidelines and paragraph 1(m) of Appendix 2 to the Circular to Licensed Corporations Licensed for Dealing in Securities - Protecting Client Assets Against Internal Misconduct dated 5 February 2016.

¹⁶ These included Windows Server 2008 and Windows Server 2012.

¹⁷ VPN creates an encrypted tunnel between user devices and the corporate network. Users can seamlessly connect to corporate applications through VPN.

other issues. Therefore, LCs' senior management should implement policies and procedures on the management and supervision of these service providers and ensure the LCs' compliance with the relevant Cybersecurity Requirements.

Moreover, a number of LCs have adopted cloud services for hosting their trading system, back-office system or both. The cybersecurity management could differ significantly for cloud-hosted systems and data from those in the traditional on-premises IT environment. Therefore, it is important for LCs to understand the cloud service models they adopt and implement the corresponding security measures.

In light of the abovementioned emerging trends and risks, we set out our expected standards on (i) phishing detection and prevention, (ii) EOL software management, (iii) remote access, (iv) Third Party Provider management and (v) cloud security in the Appendix to this circular.

Separately, we noted that SMS one-time passwords (OTPs) is one of the most common authentication factors for system login and device binding. However, there are some security concerns associated with their use, eg, fraudsters can intercept these OTPs through malware installed on the victim's mobile phones. To mitigate such risks, some LCs have adopted more secure authentication methods, such as biometrics (including facial recognition technology) and software token. LCs are reminded to keep abreast with the latest technological developments and review the risks associated with using SMS OTPs. They are also encouraged to stop using SMS OTPs for authentication and/ or implement compensating controls where appropriate.

Senior management responsibility

LCs are reminded that their senior management, in particular the MIC-IT, is ultimately responsible for the identification, monitoring and mitigation of the cybersecurity risks faced by LCs. They should:

- (a) ensure that qualified staff and Third Party Providers are appointed and adequate technology and financial resources¹⁸ are deployed to effectively manage cybersecurity risks;
- (b) review and approve cybersecurity risk management policies and procedures regularly¹⁹ to ensure that they are adequate to address the latest cybersecurity risks and threats;
- (c) ensure that cybersecurity reviews are conducted on their network and systems on a regular basis, where applicable²⁰. They should also review findings identified from these cybersecurity reviews, endorse and monitor the completion of remedial actions to ensure that issues and vulnerabilities identified are properly followed-up²¹; and
- (d) establish and maintain adequate contingency plans which address cybersecurity scenarios and corresponding contingency strategies²². These plans should be reviewed and tested regularly and revised in light of changes to the LC's operations and cybersecurity risk exposure.

¹⁸ Paragraphs 4.1 and 4.3 of the Code of Conduct.

¹⁹ Paragraphs 3.1(a) and 3.1(f) of the Cybersecurity Guidelines.

²⁰ Paragraph 3.1(e) of the Cybersecurity Guidelines.

²¹ Paragraph 3.1(e) of the Cybersecurity Guidelines.

²² Paragraph 3.1(g) of the Cybersecurity Guidelines.



The requirements in this circular take immediate effect. LCs should critically review their cybersecurity framework, procedures and controls and their systems and network to ensure they meet the expected standards of conduct. Nevertheless, the SFC recognises that some LCs may need time to update their systems to meet these requirements and the SFC will take a pragmatic approach in assessing LC's compliance.

Way forward

The existing Cybersecurity Requirements primarily focus on internet brokers, which cyber attackers frequently target. Notwithstanding, with all LCs' increasing dependence on technology for their critical operations, those engaging in non-internet trading business are equally susceptible to cyber-attacks. In this connection, in 2025, we plan to comprehensively review the existing cybersecurity requirements and expected standards, and develop an industry-wide cybersecurity framework to provide guidance to all LCs in better managing cybersecurity risks.

Should you have any queries regarding this circular, please contact your case officers-in-charge or Ms Kammy Kwok on 2231 1455.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

Enclosure

SFO/IS/004/2025