29 April 2020

Circular to licensed corporations

Management of cybersecurity risks associated with remote office arrangements

In light of the increased use of remote office arrangements, the Securities and Futures Commission (SFC) reminds licensed corporations (LCs) to assess their operational capabilities and implement appropriate measures to manage the cybersecurity risks associated with these arrangements.

When staff work remotely, they may access the LC's internal network and systems from outside the office and hold meetings through videoconferencing platforms. This circular sets out examples of controls and procedures to assist in the protection of LCs' internal networks and data. LCs are reminded that the following examples are not exhaustive. They should implement and maintain measures which are deemed appropriate to the situation and commensurate with the size and complexity of their operations[1].

(A) Remote access to internal network and systems

A recent cybersecurity incident reported by an LC showed how known vulnerabilities of Virtual Private Network (VPN) software[2] in the market could be exploited by a cyber-criminal to infiltrate the LC's network, access client data and instruct unauthorised fund transfers.

Appropriate control techniques and procedures to mitigate the cybersecurity risks associated with remote access may include:

- Implement robust VPN solutions, which provide strong encryption and two or more layers of protection, to protect the integrity of data transmitted between remote users' devices and internal systems;
- Implement multiple VPN servers for additional protection;
- Monitor, evaluate and implement security patches or hotfixes released by VPN software providers on a timely basis[3];

[1] Paragraph 4.3 of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission requires LCs to have internal control procedures and financial and operational capabilities which can be reasonably expected to protect their operations and their clients and other licensed or registered persons from financial loss arising from theft, fraud, and other dishonest acts, professional misconduct or omissions. In addition, Part IV of the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission requires LCs to ensure the integrity, security, availability, reliability and thoroughness of all information, including documentation and electronically stored data, relevant to their business operations and have operating and information management systems which meet their needs and operate in a secure and adequately controlled environment.

[2] VPNs provide an encrypted connection over the internet from a remote device to an internal network to help ensure that sensitive data is protected during transmission.

[3] Various IT security professional organisations have raised concerns about vulnerabilities in unpatched VPN software which could easily be exploited by hackers to compromise victims' networks.

- Require the use of strong passwords and implement two-factor authentication[4] for remote access logins by employees, agents and service providers, in particular when accessing privileged accounts and sensitive data repositories;

- Avoid granting standing or permanent access to external parties and only allow vendors to access specific systems during pre-determined timeframes;

- Implement different levels of remote access, such as by equipping computers and mobile devices supplied by LCs with greater capabilities than employee-owned devices;

- Implement security controls to prevent unauthorised installation of hardware and software on computers and devices provided to staff; and

- Implement robust network segmentation to segregate system servers and databases, based on criticality, to better protect more critical and sensitive data, such as clients' personal data.

(B) Use of videoconferencing platforms

Security issues with videoconferencing platforms have been reported from time to time. To mitigate the risk of unauthorised access and leakage of critical or sensitive data, appropriate control techniques and procedures may include:

- Assess the security features of videoconferencing platforms before use;

- Require participant registration for attendance in videoconferences;

- Allow only authenticated and authorised users to join the videoconference, eg, by checking their email addresses or making use of "waiting room" features[5];

- Use a random meeting ID, rather than a personal meeting ID;

- Invite participants via conferencing software or other legitimate channels, eg, office emails, and refrain from sharing links to conferences via social media posts;

- Enable the password protection feature on the videoconferencing platform;

- Lock the conference meeting once all the participants have joined, as appropriate; and

[4] Two-factor authentication refers to an authentication mechanism which utilises any two of the following factors: what a client knows, what a client has, and who a client is.

[5] "Waiting room" functions allow the host of the videoconferenceto admit only those participants who are authorised to take part.

- Use the latest version of the software with the most up-to-date security patches installed.

(C) Other measures supporting remote office arrangements

In addition, the following measures for enhancing operational capabilities and monitoring mechanisms for remote office activities should be put in place as appropriate:

System capabilities

- Assess the adequacy of, and enhance, existing information technology infrastructures, software (such as remote computer devices, network bandwidth and software licenses) and hardware (such as notebook computers and mobile devices) for the purpose of supporting remote office arrangements.

Surveillance and incident handling

- Implement monitoring and surveillance mechanisms to detect unauthorised access to internal networks and systems, such as reviewing the list of unauthorised access attempts and detecting the use of unapproved applications; and

- Develop and maintain an effective incident management and reporting mechanism.

Cybersecurity training and alerts

- Provide adequate cybersecurity training to all internal system users and issue appropriate reminders and alerts to clients, eg, advice on precautionary security measures, emerging cybersecurity threats and trends (such as phishing[6] and ransomware) and use of secure Wi-Fi networks for accessing internal networks and videoconferencing platforms, on a regular basis.

Should you have any queries regarding the contents of this circular, please contact your case officer.

Intermediaries Supervision Department
Intermediaries Division
Securities and Futures Commission

End

SFO/IS/018/2020

[6] Phishing is when hackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a fake website.