CHARLTONS

SOLICITORS

Hong Kong May 2020

SFC Guidance to Licensed Corporations on Remote Office Cybersecurity Risk Management amid COVID-19

The Securities and Futures Commission (**SFC**) issued a circular to licensed corporations regarding their cybersecurity risk management of remote office arrangements[1] on 29 April 2020 (**SFC Cybersecurity Risk Circular**) reminding SFC-licensed corporations to assess their operational capabilities and implement suitable measures to manage risks associated with remote office arrangements. The impetus for the SFC's guidance was the increased use of remote working amid the COVID-19 pandemic.

Remote working arrangements allow employees to access SFC-licensed corporations' internal networks and systems from outside the office. They also enable meetings to be held through videoconferencing. The SFC Cybersecurity Risk Circular provides non-exhaustive examples of controls and procedures to assist SFC-licensed corporations in protecting their internal networks and data.

Paragraph 4.3 of the SFC Code of Conduct for Persons Licensed or Registered with the SFC requires licensed corporations to have internal control procedures, financial and operational capabilities which are 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. Licensed corporations are thus required to implement and maintain controls and procedures that they consider appropriate to the size and complexity of their operations.

Remote Access to SFC Licensed Corporations' Internal Networks

Staff typically access SFC-licensed corporations' internal networks remotely via Virtual Private Network (**VPN**) software which provide encrypted connection over the internet allowing employees to access internal networks remotely while ensuring that sensitive data is protected during transmission. The SFC Cybersecurity Risk Circular notes a recent cybersecurity incident reported by a licensed corporation which highlighted how cybercriminals can take advantage of known defects of VPN to access SFC-licensed corporations' internal networks and client data and make unauthorised fund transfers.

Control Techniques and Procedures to Mitigate Cybersecurity Risks

The SFC Cybersecurity Risk Circular lists the following controls and procedures as means to mitigate remote access cybersecurity risks:

1. The implementation of robust VPN solutions providing strong encryption and two or more layers of protection to protect data transmitted between remote access devices and licensed corporations' internal networks;

2. Implementation of multiple VPN servers for extra protection;

[1] SFC. 29 April 2020. Circular to licensed corporations on the management of cybersecurity risks associated with remote office arrangements. Available at https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=20EC37

3. Monitoring, evaluation and implementation on a timely basis of security patches or hotfixes released by VPN software providers. IT security professionals have expressed concern that organisations with unpatched VPN software vulnerabilities may be easily hacked compromising their internal networks;

4. Requiring the use of strong passwords and two-factor authentication for remote access logins by employees, agents and service providers, especially for accessing privileged accounts and sensitive data;

5. Avoiding the grant of standing or permanent access to third parties and only permitting vendors to access specific systems during pre-determined time periods;

6. Implementation of various levels of remote access, such as ensuring that computers and mobile devices supplied by licensed corporations have better capabilities than employee-owned devices;

7. Implementation of security controls to prevent unauthorised installation of hardware and software on computers and devices provided by SFC-licensed corporations; and

8. Implementing vigorous network segmentation to segregate system servers and databases, based on criticality, to better protect critical and sensitive data, such as clients' personal data.

SFC-Licensed Corporations' Use of Video Conferencing

Videoconferencing security issues have been reported from time to time. The SFC suggests that licensed corporations use the following control techniques and procedures to reduce the risk of security breach and leakage of crucial or sensitive data:

1. Conducting a review of the security features of the videoconferencing platform before use;

2. Requiring participants to register to attend videoconferences;

3. Only permit authenticated and authorised users to participate in videoconferences such as by confirming their email addresses or using "waiting-room" features which give the videoconference host the ability to admit only those who have been authorised to take part;

4. Holding videoconferences with a random ID rather than a personal meeting ID;

5. Sending invites to participants via the videoconferencing software or other appropriate channels such as work emails and not sharing invites on social media platforms;

6. Enabling the password feature on videoconference platforms;

7. Locking videoconferences once all participants have joined; and

8. Ensuring use of the latest version of the videoconference software with updated security patches installed.

Other Remote Office Cybersecurity Risk Measures

The SFC also recommends that SFC-licensed corporations adopt the following measures to enhance operational capabilities and monitoring mechanisms for remote office arrangements:

1. System Capabilities: Assess the adequacy of, and improve, existing IT systems, software (e.g. remote computer devices, network bandwidth and software licences) and hardware (such as laptops and mobile devices) to support remote office arrangements;

2. Surveillance and Incident Handling: Put in place monitoring and surveillance mechanisms to identify unauthorised access to internal networks and systems, such as reviewing unauthorised access attempts and detecting unapproved applications use. Establish and maintain effective incident management and reporting mechanism; and

3. Cybersecurity Training and Alerts: Provide appropriate cybersecurity training to all users of the internal system and issue reminders and alerts to clients on a regular basis on issues such as cybersecurity threats and trends on phishing[2] and ransomware,[3] and the use of secure Wi-Fi networks to access internal network and for videoconferencing platforms.

[2] Phishing occurs 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.

[3] A type of malware that encrypts files which makes them inaccessible and demands a ransom payment to decrypt them.

With the rise of work from home arrangements amid the COVID-19 pandemic, remote office arrangements may become more prevalent and SFC-licensed corporations should assess and review their cybersecurity controls and measures to ensure they are compliant with the applicable laws and rules.

The SFC invites licensed corporations to contact their case officers if they have any questions on issues raised in the circular.

CHARLTONS

Award winning Hong Kong law firm

This newsletter is for information purposes only.

Its contents do not constitute legal advice and it should not be regarded as a substitute for detailed advice in individual cases.

Transmission of this information is not intended to create and receipt does not constitute a lawyer-client relationship between Charltons and the user or browser.

Charltons is not responsible for any third party content which can be accessed through the website.

If you do not wish to receive this newsletter please let us know by emailing us at unsubscribe@charltonslaw.com

Hong Kong Office
Dominion Centre
12th Floor
43-59 Queen’s Road East
Hong Kong
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596

www.charltonslaw.com