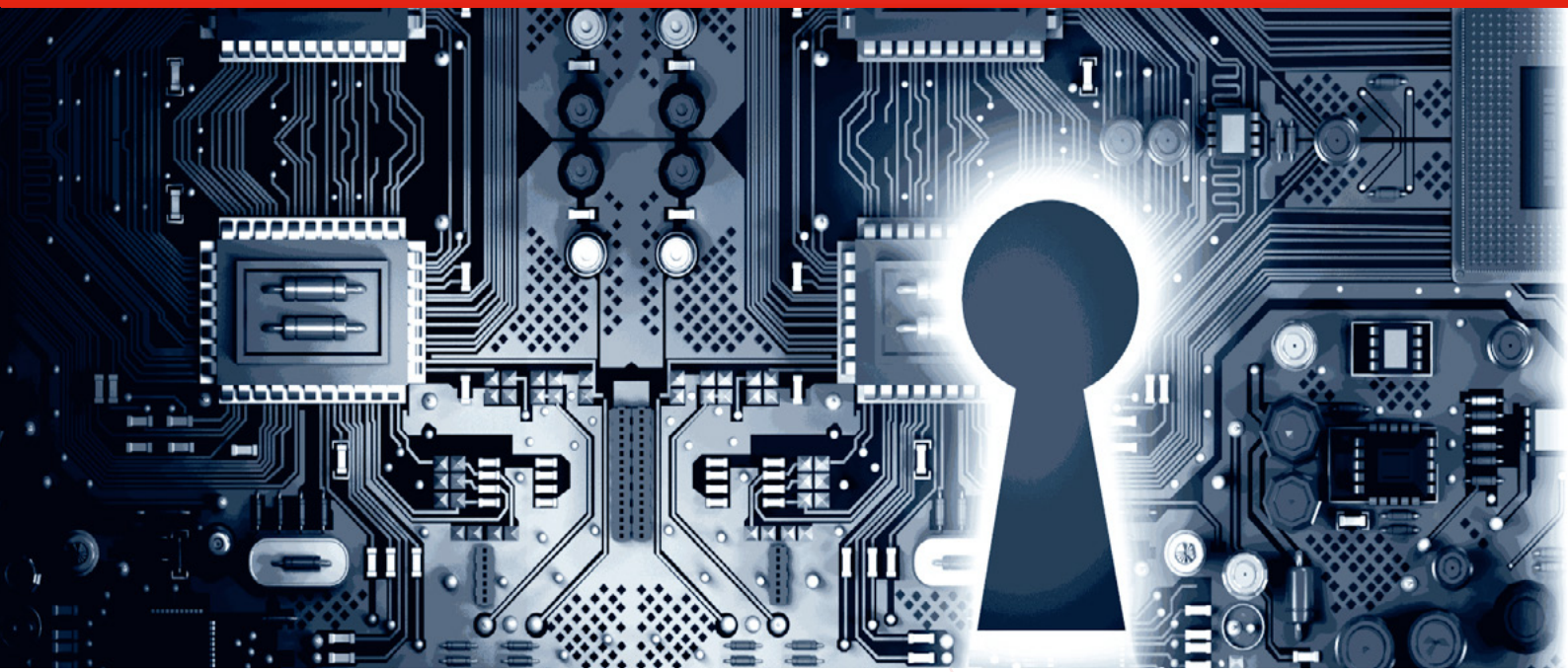

Hong Kong SFC Fines Luk Fook Securities HK$2.1 Million for Cybersecurity Failures

Hong Kong's Securities and Futures Commission (**SFC**) has reprimanded and fined SFC-licensed corporation Luk Fook Securities (HK) Limited (**LFSHK**) HK$2.1 million for failing to implement adequate and effective cybersecurity controls in breach of the SFC's Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (**SFC Code of Conduct**) and Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (**SFC Cybersecurity Guidelines**). According to the SFC's Statement of Disciplinary Action, these failings may have contributed to LFSHK's inability to withstand a ransomware attack on 19 September 2022 and caused an approximate three-week delay in the recovery of its systems. The SFC's action was taken under section 194 of the Hong Kong Securities and Futures Ordinance (**SFO**).

Ransomware Attack on SFC Licensed Corporation

LFSHK informed the SFC and its clients of the ransomware attack on the day of the attack which had affected LFSHK's critical IT infrastructure, including its file servers, domain controllers, email servers, trading application servers and accounting servers. System restoration was carried out in stages and full recovery was completed only on 7 October 2022. However, there was no evidence of misappropriation of client assets, unauthorised trading, client financial loss or client information leakage, and no client complaints were made.

After the incident, LFSHK engaged an external consultant to investigate and advise on the incident. At the SFC's request, it also appointed an independent reviewer to assess the incident and conduct a regulatory review of LFSHK's cybersecurity-related internal controls and remediation measures. The SFC conducted a separate investigation into LFSHK's conduct.

Key Cybersecurity Failures Identified by the SFC

The investigations identified a series of specific failings in LFSHK's cybersecurity systems:

- **Insufficient network security controls:** a number of LFSHK's network devices lacked firewall protection and were not monitored by a Security Information and Event Management (SIEM) tool, leaving the network exposed and enabling the attacker to access an internal system directly from the internet.
- **Inadequate user access and privileged account management:** LFSHK lacked effective controls over

user access and privileged accounts. Credentials for third-party vendors and staff were cached in remote support instances, increasing the risk of compromise and lateral movement within the network.

- **Use of unsupported legacy systems:** the infected VMware[1] environment ran outdated operating systems (Microsoft Windows Server 2008 and Windows 7), which no longer receive security updates and are incompatible with modern endpoint protection, leaving critical vulnerabilities unpatched.

- **Outdated antivirus protection:** antivirus signatures on the Active Directory server were approximately one year out of date, undermining the firm's ability to detect and prevent malware such as ransomware.

- **Inadequate controls over remote access:** LFSHK did not implement sufficient controls for remote access, including strong (e.g. two-factor) authentication, proper access restrictions, device security or remote device management, increasing the risk of unauthorised access and delayed incident detection.

- **Poor password management practices:** there were no effective password policies or related training, and system account credentials were stored in an unencrypted Excel file on the Active Directory server — a critical vulnerability the attacker likely exploited to further compromise the network.

- **Lack of controls over external device security:** LFSHK did not restrict or monitor the use of USB devices, allowing users to connect external storage devices without oversight and exposing the network to the risk of malware introduction and propagation.

- **Insufficient cybersecurity awareness training:** the firm's last cybersecurity training session was held in 2018 and covered only two-factor authentication for the trading system, with no further training or updates provided since, leaving staff unprepared for evolving cyber threats.

The SFC's Disciplinary Statement also noted that LFSHK's recovery was slowed by further weaknesses in its backup and continuity arrangements. Daily data backups were stored on an external hard drive that was not consistently disconnected from the network, meaning the backup files themselves were compromised in the attack and could not be relied upon for recovery. In addition, the firm's business continuity plan did not address specific scenarios such as ransomware attacks or data loss and had not been subject to regular review or updates. Following the incident, and throughout the recovery period, LFSHK had also not yet established policies and procedures addressing key areas of cybersecurity risk, such as incident management, data security and record retention.

The firm's remote working arrangement during the COVID-19 pandemic also formed part of the factual background. LFSHK had implemented a VMware virtualised environment running Windows 7 to allow staff to access office workstations remotely, and this environment was also used by third-party vendors and the IT department for support. The hacker exploited that remote access setup and gained access to the Active Directory server, likely through a cached remote desktop shortcut. The SFC noted that its 29 April 2020 circular, *Management of Cybersecurity Risks Associated with Remote Office Arrangements*, had highlighted the risks associated with remote access and working arrangements and set out suggested control techniques to mitigate them, underscoring that LFSHK's failings occurred against a backdrop of specific regulatory guidance.

LFSHK's Cybersecurity Breaches: The SFC's Findings

The SFC found that LFSHK committed misconduct in failing to comply with fundamental cybersecurity measures required under the SFC Code of Conduct and SFC Cybersecurity Guidelines, which likely contributed to its inability to withstand the ransomware attack and delayed its recovery.

In particular, LFSHK's failures breached General Principle 2 (Diligence), General Principle 3 (Capabilities) and General Principle 7 (Compliance), paragraph 12.1 (Compliance: in general), paragraph 18.5 (Adequacy of system) and paragraphs 1.1.4, 1.2.4(a), 1.2.4(b), 1.2.4(c), 1.2.4(d), 1.2.6(b) and 1.2.7 and 1.2.8(a) of Schedule 7 (Additional requirements for licensed or registered persons conducting electronic trading) of the SFC Code of Conduct. It also breached the following paragraphs of the SFC Cybersecurity Guidelines Paragraphs: 2.1 (Deploy a secure network infrastructure), 2.2 (User access management), 2.3 (Security controls over remote connection), 2.4 (Patch management), 2.5 (End-point protection), 2.6 (Unauthorised installation of hardware and software), 2.8 (System and data backup), 2.9 (Contingency planning for cybersecurity scenarios) and 3.3 (Cybersecurity awareness training).

1 VMware was an older system environment mainly used by external system vendors for maintenance and by a small group of internal users to access the trading system. Although both groups operated within the same VMware environment, their access was restricted to separate areas. System vendors could access the control panel, while internal users could only access the trading system.

Mitigating Factors and SFC's Determination of Sanctions

In deciding the sanction, the SFC took into account that LFSHK had reviewed the incident to identify the root causes and extent of its failings, and appointed an independent reviewer at SFC's request. Additionally, it had taken remedial steps to strengthen its controls while cooperating with the SFC and had a clean disciplinary record. Finally, the SFC took into account that there was no evidence of loss to clients.

Even with those mitigating factors, the regulator still considered a public reprimand and a HK$2.1 million fine appropriate. The case is a reminder that cyber resilience is a core compliance issue for licensed corporations.

CHARLTONS
易周律师行

Hong Kong Office

Dominion Centre 12th Floor
43-59 Queen's Road East Hong Kong

enquiries@charltonslaw.com

www.charltonslaw.com
Tel: + (852) 2905 7888
Fax: + (852) 2854 9596