waystone | Compliance Solutions

SFC's Cyber Security Review of Licensed Corporations

Leo Wong July 18, 2025

The Hong Kong Securities and Futures Commission (hereinafter the "SFC") released its 2023/24 Thematic Cyber Security Review of Licensed Corporations (hereinafter "LCs") in February 2025, assessing internet brokers' adherence to the SFC's Cybersecurity Guidelines and Code of Conduct.

The report details eight major cyber security incidents from 2021 to 2024, identifies prevalent vulnerabilities, and sets forth expected standards for LCs, particularly fund managers, to safeguard client data, ensure operational continuity, and uphold market integrity in Hong Kong's evolving digital financial landscape. It also highlights the SFC's future initiatives to bolster industry-wide cyber security, drawing parallels with governance principles from climate risk and fund management compliance.

Understanding Cyber Security

Cyber Security is vital for Licensed Corporations, in particular Type 9 fund managers, who manage sensitive client data and significant assets. The SFC highlights risks such as ransomware and unauthorised access that can disrupt operations, erode investor trust, and invite regulatory scrutiny. Aligning with SFC priorities, such as risk management and senior oversight, robust cyber security compliance helps LCs avoid penalties while boosting competitiveness by appealing to security-conscious investors.

The SFC's 2021–2024 review of eight major cyber security incidents affecting LCs, particularly internet brokers, revealed:

Incidents: ransomware disrupted trading and back-office systems; unauthorised account access enabled fraudulent trades; third-party IT vendor breaches caused operational issues.

Vulnerabilities: use of outdated or end-of-life (EOL) software, weak encryption, inadequate 2FA, lax server/firewall controls, delayed patches, excessive user access, and insufficient senior management oversight.

Findings: despite some improvements, persistent deficiencies underscore the need for stronger cyber security controls.

Expected Standards and Recommendations

Phishing detection and prevention: phishing attacks are a major threat to LCs, with many facing incidents, including a ransomware attack from a phishing email. Weak anti-malware and lack of training increase risks. LCs should deploy updated anti-malware, avoid email/SMS hyperlinks, and conduct quarterly phishing simulations, supported by email filtering, sandboxing, and reporting channels.

EOL software management: half of LCs use EOL software such as Windows 7, lacking IT asset policies, leading to incidents. Organisations must create IT asset policies, conduct annual inventories, plan upgrades, and avoid EOL software on critical systems, using spreadsheets, automated tools, and CIO-led remediation.

Remote access: unpatched VPNs/RDPs, exploited in attacks such as Lockbit, and missing 2FA expose LCs to risks. Implement VPNs with 2FA, session timeouts, third-party monitoring, and SFC compliance, using virtual desktop restrictions, remote wipe, and IP whitelisting.

Third-Party provider management: poor third-party provider management, with weak due diligence and SLAs, causes breaches. LCs should perform due diligence, set cyber security SLAs, maintain provider lists, and plan contingencies, using questionnaires, SOC2 reviews, and annual drills.

Cloud security: cloud security is weak in 60% of LCs due to poor access controls and encryption. Strengthen cloud security with role-based access, data encryption, and regular audits to ensure data protection and compliance.

Implications for Fund Managers

Fund managers face heightened cyber security expectations due to their management of client assets and sensitive data, necessitating robust oversight of third-party IT vendors through due diligence and strong SLAs, secure VPNs with 2FA for remote access, and updated encryption and End-of-Life software to protect client information. To comply with SFC standards, they should ensure the due diligence conducted on any third-party IT vendors are adequate, maintain and update policies on the prevention of cyber security, perform cyber security risk assessment on the LC, aligning with broader SFC compliance goals such as managing conflicts in private funds.

How can Waystone help?

Waystone Compliance Solutions is a leading provider of cyber security consulting and compliance services to the financial services industry. If you would like to find out how Waystone can help you to assess your current cyber security measures, please reach out to your usual Waystone representative, or contact us below.

Get in touch →