New SFC Requirements for Cybersecurity to Counter AI-enabled Cyber Threats

With ever increasing numbers of cyberattack incidents in Hong Kong and the heightened risk posed by frontier artificial intelligence (**AI**) models, the SFC issued a Circular to Licensed Corporations, SFC-licensed Virtual Asset Service Providers and Associated Entities: Enhanced Cybersecurity Measures to Address Evolving Risks Arising From Artificial Intelligence-enabled Cyberattacks requiring SFC-licensed corporations and virtual asset service providers (**VATPs**) and their associated entities (together, **SFC-licensed firms**) to review and improve their cybersecurity measures to meet evolving threats. The circular, issued on 2 June 2026, highlights the responsibility of SFC-licensed firms' senior management, including the Manager-in-Charge of Information Technology, for managing firms' cybersecurity risks and requires Managers-in-Charge of Information Technology to ensure the review, approval and implementation of improvements to firms' cybersecurity measures to safeguard their operations and protect clients' interests. Where necessary, firms are expected to appoint IT security expects to advise them.

The circular's Appendix sets out illustrative examples of suggested controls and procedures for each of the cybersecurity areas covered in the circular. Licensed firms conducting electronic trading, particularly large retail brokers, depositaries of SFC-authorised collective investment schemes (i.e. corporations licensed for Type 13 regulated activity) and VATPs are expected to implement all the measures set out in the Appendix, whereas other SFC-licensed firms are expected to take them into consideration depending on the nature, scale and complexity of their businesses, their dependency on technology and exposure to cybersecurity risks.

Developments in AI-enabled Cyber Threats to SFC-licensed Corporations & VATPs

Frontier AI models have advancing ability to plan and execute complex actions autonomously and can spot security flaws undetected by software developers (**zero-day vulnerabilities**). They are also capable of identifying multiple vulnerabilities which would cause minimal impact to the firm if exploited, and then chaining them together to exploit a system in ways that can result in significant disruptions. Operation across multiple interconnected systems and large-scale attacks on these systems are also enabled by AI.

Developments in AI-enabled tools may also significantly lower the technical barrier for threat actors to execute various malicious activities, including phishing, social engineering, deepfake impersonation and reconnaissance. With these elevated levels of speed and scale in cyberattacks, SFC-licensed firms are advised to ensure that their cyberattack prevention, detection, response and recovery measures are effective.

Greater availability of low-cost AI-enabled tools is expected to increase the number and frequency of security patches and updates from major software sellers. Simultaneously, the time interval between vulnerability identification or disclosure and its exploitation by threat actors is rapidly diminishing. Given the compressed response time, the SFC suggests that SFC-licensed firms should enhance and expedite patching and vulnerability management processes to minimise firms' exposure to potential cyberattacks.

SFC-licensed Firms: Measures to Address Risks of AI-enabled Cyberattacks

The SFC expects licensed corporations and VATPs to implement robust security controls to protect their systems against attack and prevent unauthorised access to confidential client information and misappropriation of client assets. They should, in particular maintain an accurate and up-to-date inventory of their technology assets and components, identify those that are externally exposed, business critical or dependent on third party components, and promptly direct protective measures to the highest-risk areas.

The circular additionally reminds SFC-licensed firms using AI language models that these can amplify existing cyber risks and introduce additional risks that can be exploited or triggered during an AI-assisted cyberattack. These include risks arising from adversarial attacks against AI language models, data leakage and system prompt override. SFC-licensed firms should ensure that the associated cybersecurity risks are addressed in the firms' cybersecurity framework (as set out below) and incident handling arrangements, taking into account the core principles in the Circular to Licensed Corporations – Use of Generative AI Language Models (**AI Circular**). Further, licensed firms intending to adopt AI language models in their high-risk use cases (i.e., as identified under paragraph 8 of the AI Circular) must comply with the notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules.

SFC-licensed Firms: Cybersecurity Framework

The SFC sets out 5 areas in which licensed firms should enhance their cybersecurity measures. Illustrative examples of suggested controls and procedures in each area are set out in the circular's Appendix.

1. Patching and Vulnerability Management

SFC-licensed firms should take prompt actions to address known vulnerabilities. Additionally, adequate procedures for handling urgent and critical fixes falling outside routine patching cycles should be implemented, especially for vulnerabilities affecting their business critical components. Sufficient resources should be allocated to effectively handle any potential surge in patching demands.

2. Access and Privilege Controls

Licensed firms should design their system controls based on the assumption that any user, device, privileged account or network component may be compromised, and they should implement robust access and privilege controls and minimise attack surfaces. In particular, to reduce the risk that untrusted inputs or unauthorised users may manipulate systems, the SFC advises licensed firms to:

a. enforce least-privilege access to all business critical components, including limiting connectors and tool permissions to what is necessary for the intended use case and implement measures to safeguard privileged accounts (i.e., accounts with elevated rights allowing them to access a firm's network, systems, servers and devices and to, among other things, modify system configurations, manage other user accounts and account rights and revise client data);

b. enhance firewalls and network segmentation, preferably a micro network segmentation where feasible to limit lateral movement capabilities across networks and systems;

c. treat external and untrusted inputs as potentially adversarial and prevent such inputs from directly altering system instructions or triggering privileged actions; and

d. apply maker-checker controls for high-impact actions.

3. Detection and Monitoring Measures

SFC-licensed firms are expected to improve their threat detection and monitoring of anomalies in client trading activities and system activities to ensure they are commensurate with the evolving threat environment. Threat intelligence gathering capability should also be enhanced.

4. Third-party Supply Chain Risk Management

There could be AI-enabled threats targeting third-party service providers that support the critical operations and business critical components of SFC-licensed firms. Licensed firms should therefore strengthen their third-party supply chain risk governance framework and enhance initial and ongoing assessments on third-party service providers.

5. Incident Response and Recovery

Effective incident handling procedures and contingency plans are crucial to prevent AI-enabled cyberattacks from leading to unauthorised access to firms' networks and systems, leakage of sensitive information, and significant disruption of firms' services. As traditional detection and response processes may no longer be able to handle AI-enabled attacks, licensed firms are advised to establish adequate escalation and reporting mechanisms and consider pre-planned containment and exploit-interruption strategies, including the ability to block malicious activities, isolate affected systems and restrict access rapidly.

Licensed firms are also advised to:

- regularly test their cybersecurity incident handling procedures and contingency plans through tabletop exercises and simulated attacks to assess the effectiveness of these plans;
- back up business records, client and transaction databases, and supporting documentation on a regular basis and implement proper measures to ensure the availability of the backup copies. Licensed corporations conducting electronic trading and VATPs are already required to back up these records and data at least daily; and
- promptly notify the SFC of material cybersecurity incidents and attacks as required under the Paragraph 12.5(e) of the Code of Conduct and Paragraphs 16.7(b) and (c) of the Guidelines for Virtual Asset Trading Platform Operators.

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