SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

Circular

2 June 2026

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

1. In light of the evolving cyber threat landscape with an increase in the number of cybersecurity incidents[1] in Hong Kong and heightened cyberattack risks posed by frontier artificial intelligence (AI) models, the Securities and Futures Commission (SFC) wishes to remind licensed corporations (LCs), SFC-licensed virtual asset service providers (VATPs) and their associated entities (collectively referred to as "licensed firms") to review and enhance their cybersecurity measures to address these evolving threats.

2. The SFC has been engaging licensed firms and key internet trading platform providers on their preparedness for cyberattacks that may be assisted or accelerated by AI-enabled tools. This circular highlights the observations from these engagements and provides practical guidance to help licensed firms in enhancing their resilience and response strategies.

3. Licensed firms should assess their preparedness for AI-enabled cyberattacks, take appropriate actions to address any vulnerabilities in their existing systems and enhance their cybersecurity measures to better safeguard their operations and protect client interests. They are reminded that their senior management, including the Manager-in-Charge of Information Technology (MIC-IT), is ultimately responsible for managing cybersecurity risks faced by their firms. In particular, the MIC-IT should ensure that changes to the firm's cybersecurity framework are adequately reviewed and approved and that enhancements to the firm's cybersecurity measures are implemented properly and promptly. Licensed firms should seek advice and assistance from IT security experts as necessary.

Developments in AI-enabled cyber threats

4. Recent developments in AI capabilities may significantly reduce the expertise, cost, and time needed to identify and exploit vulnerabilities in critical software and infrastructure. In particular, licensed firms should take note of the following developments:

   - *Increase in sophistication and frequency of cyberattacks*: Frontier AI models are advancing rapidly, demonstrating an unprecedented ability to plan and execute complex, multi-step actions autonomously. For example, these models are becoming more capable of identifying security flaws which have so far remained undetected by

[1] According to the Hong Kong Computer Emergency Response Team Coordination Centre, the number of cybersecurity incidents (including botnet, distributed denial-of-service, defacement, malware and phishing) increased to 15,877 in 2025 from 12,536 in 2024.

software developers (so-called “zero-day vulnerabilities”). They are also capable of systematically identifying multiple “lower risk-rated” vulnerabilities[2] and chaining them together to exploit a system in ways that can result in significant, high-impact disruptions. Furthermore, they can operate across multiple interconnected systems and orchestrate large-scale attacks on these systems.

The proliferation of AI-enabled tools may also significantly lower the technical barrier for threat actors to execute various malicious activities, such as phishing, social engineering, deepfake impersonation, and reconnaissance.

These developments introduce new dimensions of speed and scale to potential cyberattacks and it is envisaged that licensed firms, their staff and their clients will be subject to more frequent and targeted attacks. Licensed firms should therefore review whether their existing cyberattack prevention, detection, response and recovery procedures remain effective.

- *Reduced response time for implementing remedial measures to minimise exposure to potential cyberattacks*: The increasing availability of low-cost AI-enabled tools allows rapid identification of new vulnerabilities. This is expected to significantly increase the volume and frequency of security patches and updates released by major software vendors. Moreover, the time interval between the identification or disclosure of a vulnerability and its exploitation by threat actors is rapidly diminishing with the availability of these AI tools.

  Patching and change management processes typically involve multiple steps, including coordination with software vendors, testing, deployment, and review, and require time to complete. Licensed firms should therefore enhance and expedite their patch and vulnerability management processes to minimise the window of exposure to potential attacks.

Measures to address potential AI-enabled cyberattack risks

5. Licensed firms are expected to implement robust and up-to-date security controls to protect their systems against potential threats, prevent confidential client information from unauthorised access or disclosure and safeguard client assets against misappropriation caused by cyberattacks.

6. As a foundation, licensed firms should maintain an accurate and up-to-date inventory of their technology assets and components, including hardware, software, network infrastructure, databases and cloud services. Firms should identify which assets and services are externally exposed, business-critical (referred to as “business critical components”), or dependent on third-party components, so that remediation and protective measures can be directed to the highest-risk areas promptly and effectively. Furthermore, given the high speed at which frontier AI models can identify exploitable weaknesses, licensed firms should ensure that their asset inventories are kept sufficiently up-to-date to facilitate same-day prioritisation and containment decisions when new vulnerabilities or threat intelligence emerge.

---

2 “Lower risk-rated” vulnerabilities refer to vulnerabilities which, if exploited, would result in minimal impact on the firm.

7. As vulnerabilities can now be identified and exploited at a faster pace, licensed firms should review and enhance their cybersecurity frameworks to ensure they remain appropriate and effective in preventing, detecting, responding to and recovering from evolving threats. They are expected to consider the areas mentioned under sections (A) to (E) below when reviewing and enhancing their frameworks. Examples of controls and procedures are set out in the Appendix to assist licensed firms in managing and mitigating potential risks associated with AI-enabled cyberattacks.

8. In addition, licensed firms are reminded that the use of AI language models in their operations, regardless of whether the model is developed internally, provided by a group company or a third-party service provider, or obtained from an open source, may 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. Therefore, these licensed firms should ensure that the associated cybersecurity risks are addressed in their cybersecurity framework and incident handling arrangements, taking into account the core principles set out in November 2024 Circular[3]. Separately, licensed firms which intend to adopt AI language models in their high-risk use cases[4] are reminded of their obligation to comply with the notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules[5].

(A) Patching and vulnerability management

9. Licensed firms should review and enhance their patching and vulnerability management processes. They should take prompt actions to address known vulnerabilities and implement adequate policies and procedures for handling urgent and critical fixes that fall outside routine patching cycles, especially for vulnerabilities and fixes affecting their business critical components. They should also allocate sufficient resources to effectively handle any potential surge in patching demands.

(B) Access and privilege controls

10. Licensed firms should design system controls based on the assumption that any user, device, privileged account or network component may be compromised[6]. In particular, they should implement robust access and privilege controls and minimise attack surfaces.

11. To reduce the risk that untrusted inputs or unauthorised users may manipulate systems or workflows, licensed firms should:

    (i) 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 adequate measures to safeguard privileged accounts[7];

---

3 Circular to licensed corporations - Use of generative AI language models dated 12 November 2024 (November 2024 Circular).
4 Paragraph 8 of the November 2024 Circular.
5 Paragraph 30 of the November 2024 Circular.
6 A network which follows this design principle may be referred to as a “zero-trust network”, under which access is not implicitly trusted based solely on network location or user status.

(ii) enhance firewalls and network segmentation. In particular, licensed firms should implement micro network segmentation where feasible to limit lateral movement capabilities across networks and systems;

(iii) treat external and untrusted inputs, including content retrieved from apps, emails, documents and webpages, as potentially adversarial and prevent such inputs from directly altering system instructions or triggering privileged actions; and

(iv) apply maker-checker controls for high-impact actions.

(C) Detection and monitoring measures

12. Licensed firms should strengthen their threat detection and monitoring of anomalies in client trading activities and system activities to ensure they are commensurate with the evolving threat environment. They should also improve their threat intelligence gathering capability.

(D) Third-party supply chain risk management

13. Licensed firms should implement proper procedures to address AI-enabled threats targeting third-party service providers that support their critical operations and business critical components (third-party service providers). They should strengthen their third-party supply chain risk governance framework, enhance initial and ongoing assessments on third-party service providers to factor in the latest threat landscape and ensure the proper management of cybersecurity risks associated with third-party service providers, particularly those arising from AI-enabled cyberattacks.

(E) Incident response and recovery

14. Licensed firms should review and enhance their cybersecurity incident handling procedures and contingency plans to effectively handle AI-enabled cyberattacks that may lead to, among other things, unauthorised access to their networks and systems, leakage of sensitive information, and significant disruption of services.

15. Licensed firms should recognise that AI-enabled attacks may unfold faster than traditional detection-and-response processes can handle. As a result, reliance on post-incident investigation, or on issues being escalated through normal channels, may allow the attack to continue or the situation to worsen before effective action is taken. Firms should therefore 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.

16. Licensed firms should regularly test their cybersecurity incident handling procedures and contingency plans through tabletop exercises, simulated attacks or other appropriate means to assess the effectiveness of these procedures and plans.

---

[7] This refers to 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.

17. Licensed firms should back up business records, client and transaction databases, and supporting documentation on a regular basis[8] and implement proper measures to ensure the availability of the backup copies.

18. Licensed firms should also promptly notify the SFC of material cybersecurity incidents and attacks as required under the Code of Conduct[9] and the VATP Guidelines[10].

Way forward

19. The SFC will continue to monitor developments in this area and maintain close dialogue with the industry, key technology service providers and other regulators. The SFC may issue further guidance, conduct reviews to assess licensed firms' preparedness and resilience in responding to cybersecurity incidents, or take supervisory action where appropriate, in light of the evolving risks.

20. Should you have any queries regarding this circular, please contact your case officer-in-charge.

Intermediaries Division
Securities and Futures Commission

Enclosure

End

SFO/IS/020/2026

8 LCs engaged in electronic trading (see paragraph 18.2(d) of the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission (Code of Conduct)) and VATPs are required to back up such records and data at least on a daily basis.
9 Paragraph 12.5(e) of the Code of Conduct.
10 Paragraphs 16.7(b) and (c) of the Guidelines for Virtual Asset Trading Platform Operators (VATP Guidelines).