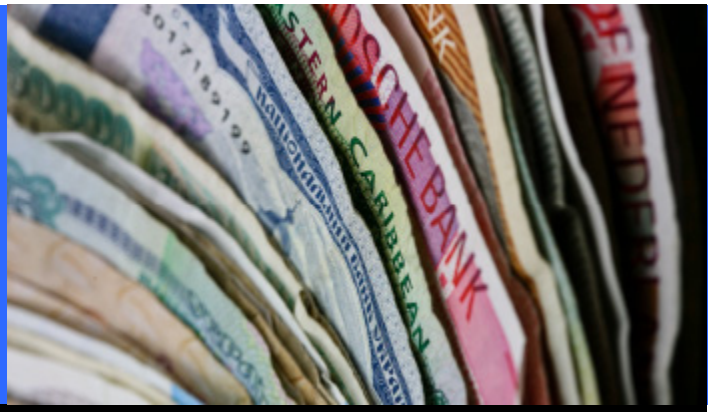
View on our website.

GIBSON DUNN



Financial Regulatory Update June 10, 2026

Hong Kong Regulators Call for Strengthened Cyber Resilience Against AI-Enabled Cyber Threats

The SFC and HKMA Circulars are especially relevant to licensed firms and banks engaging in electronic trading (particularly large retail brokers and depositaries of SFC-authorized collective investment schemes licensed for Type 13 regulated activity) as well as VATPs.

On June 2, 2026, the Securities and Futures Commission (**SFC**) issued a circular to licensed corporations, SFC-licensed virtual asset service providers (**VATPs**) and their associated entities (collectively referred to as **licensed firms**), reminding them to review and enhance their cybersecurity measures in light of heightened risks posed by artificial intelligence (**AI**)-enabled cyberattacks (**SFC Circular**).[1] On the same day, the Hong Kong Monetary Authority (**HKMA**) issued a circular to all authorized institutions, urging vigilance against AI-powered cyber threats (**HKMA Circular**), reflecting a parallel focus on cybersecurity resilience within the banking sector.[2]

The SFC and HKMA Circulars are especially relevant to licensed firms and banks engaging in electronic trading (particularly large retail brokers and depositaries of SFC-authorized collective investment schemes licensed for Type 13 regulated activity) as well as VATPs. The circulars come against the backdrop of a sharp rise in cyber incidents in Hong Kong, which the SFC notes increased by 27% to 15,877 in 2025 (from 12,536 in 2024) according to the Hong Kong Computer Emergency Response Team Coordination Centre. This client alert outlines the key expectations of the SFC and HKMA regarding measures to mitigate potential AI-enabled cyberattack risks.

I. Developments in AI-Enabled Cyber Threats

Both regulators share the view that frontier AI models mark a qualitative shift in the cyber threat landscape. In particular, these models are becoming more capable of planning and executing complex, multi-step actions autonomously, identifying security flaws which have so far remained undetected by software developers (so-called "zero-day vulnerabilities"), chaining multiple lower risk-rated vulnerabilities together, and operating across interconnected systems.

This changes the risk calculus for firms in two important ways. First, by automating the discovery and chaining of vulnerabilities, frontier AI models significantly lower the technical barrier to entry, enabling a wider range of threat actors to execute sophisticated malicious activities (such as phishing and deepfake impersonation). Second, the increasing availability of frontier AI models also means existing security defences may no longer be adequate at their current calibration. Specifically, the time between the disclosure or identification of a vulnerability in security software and its exploitation may become significantly shorter, making traditional patching and change management timelines less effective.

II. Key Regulatory Expectations

In light of the escalating cyber risks from frontier AI models, both the SFC and the HKMA expect licensed firms and authorized institutions to enhance internal controls. Below is a summary of the key requirements organized by theme, drawing from both the SFC and HKMA Circulars.

Areas of focus	**Requirements from the SFC Circular**	**Requirements from the HKMA Circular**
Cybersecurity controls and resilience enhancements	<u>Patching and vulnerability management</u> Licensed firms review and enhance their patching and vulnerability management processes. This includes: • taking prompt action to address known vulnerabilities; • implementing adequate policies and procedures for urgent and critical fixes outside routine patching cycles, especially in relation to business critical components; and • allocating sufficient resources to handle a potential surge in patching	Authorized institutions are already expected to have multi-layered defenses against zero-day vulnerabilities targeted by frontier AI-models (such as appropriate patching protocol) pursuant to the HKMA's existing supervisory requirements. In view of the evolving threat, authorized institutions are expected to assess whether current arrangements remain fit-for-purpose assuming that the scale and speed of attacks will accelerate with frontier AI's assistance. Additionally, authorized institutions that have implemented a Secure

	demands, particularly for vulnerabilities affecting business-critical components. <u>Access and perimeter controls</u> Licensed firms should design system controls on the assumption that any user, device, privileged account or network component may be compromised. In particular, they should: • enforce least-privilege access to all business critical components; • enhance firewalls and network segmentation; • treat external and untrusted inputs (e.g., contents from apps, emails, documents and webpages) as potentially adversarial and do not allow them to alter system instructions or trigger privileged actions directly; and • apply maker-checker controls for high-impact actions. <u>Detection and monitoring</u> Licensed firms should strengthen threat detection and monitoring of anomalies in client trading activities and system activities and improve their threat intelligence gathering capability.	Tertiary Data Backup (**STDB**) should consider whether and how those arrangements could be improved to enhance response capacity in the event of a destructive attack. Authorized institutions that have not implemented STDB should revisit that decision in light of the evolved risk landscape.
Third-party supply chain risk management	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**). Specifically, they should:	Authorized institutions should assess the cyber resilience capabilities of third party service providers, which as common “nodes” supporting the ecosystem, are increasingly being targeted by threat actors.

	• 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 proper management of cybersecurity risks associated with third party service providers, especially those arising from AI-enabled cyberattacks.	
Incident response and recovery	• Licensed firms should review and enhance incident handling procedures and contingency plans for AI-enabled cyberattacks that may result in unauthorized access, leakage of sensitive information or significant service disruption. • Since AI-enabled attacks may outpace traditional detection-and-response processes, the SFC expects licensed firms 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 should regularly test their cybersecurity incident handling procedures and contingency plans through tabletop exercises, simulated attacks or other appropriate methods to assess the effectiveness of these procedures and plans. • Licensed firms should regularly back up business records, client and	The HKMA warns that as the velocity and intensity of cyberattacks trend upwards, breach scenarios will become more probable. Therefore, authorized institutions should: • review the readiness of their incident response and recovery processes, including playbooks for prominent cyberattacks; • conduct scenario testing where appropriate, including as part of existing operational resilience programs; and • ensure that any third parties that are dependent on the response and recovery process are equipped and sufficiently resourced to step up in times of need.

	transaction databases, and supporting documentation, and implement appropriate measures to ensure the availability of those backup copies. • Licensed corporations engaged in electronic trading and VATPs are required to back up such records and data at least on a daily basis. • Licensed firms are reminded to notify the SFC promptly of material cybersecurity incidents and attacks.	

The SFC Circular also includes an appendix setting out a non-exhaustive list of recommended controls and procedures to assist licensed firms to reviewing and enhancing their cybersecurity framework, and in managing and mitigating risks associated with AI-enabled cyberattacks (**Appendix**).[3] While these measures are illustrative and should be implemented having regard to the licensed firm's nature, scale, complexity, technology dependencies and cyber risk exposure, the SFC indicates that certain firms, such as those engaged in electronic trading (particularly large retail brokers, depositaries of SFC-authorized collective investment schemes licensed for Type 13 regulated activity) and VATPs are generally expected to implement all of the measures in the Appendix.

More fundamentally, the SFC also expects licensed firms to maintain an accurate and up-to-date inventory of technology assets and components – including hardware, software, network infrastructure, databases and cloud services – and to identify assets and services that are externally exposed, business-critical or dependent on third-party components, so that remediation and protective measures can be directed to the highest-risk areas promptly and effectively. Licensed firms should also ensure that their asset inventories are kept sufficiently up-to-date to facilitate same-day prioritization and containment decisions when new vulnerabilities or threat intelligence emerge.

By contrast, the HKMA Circular does not specify particular controls or measures to be implemented. Instead, it largely builds on and refers authorized institutions to comply with existing supervisory requirements and emphasizes the need for authorized institutions to critically review whether their current controls remain fit-for-purpose in light of evolving AI-enabled threats. The HKMA also places particular focus on testing and validation—such as assessing incident response and recovery readiness through scenario testing, and evaluating third-party resilience.

III. Regulatory Initiatives Going Forward

Both the SFC and HKMA have stated that they will continue monitoring developments, maintain dialogue with the industry and relevant stakeholders, and provide additional guidance to the

industry. Notably, the HKMA has also stated that it will continue to support the following targeted initiatives:

- the establishment of a task force on AI-driven cyber risks as an official forum for key stakeholders in the financial and cyber risk ecosystem to facilitate information sharing and discussion of practical ecosystem responses;
- the development of the Cyber Resilience Testing Framework aimed at assisting authorized institutions in stress testing their ability to respond to and recover from actual breach situations, with an initial test run involving selected institutions targeted for late 2026;
- supporting the implementation of the Protection of Critical Infrastructures (Computer Systems) Ordinance (**PCICSO**) by entering into a Memorandum of Understanding with the Commissioner of Critical Infrastructure (Computer-system Security) to ensure a coordinated approach to implementation, while prioritizing a reduction in compliance burdens for the industry where practicable;[4] and
- issuing a Sectoral Code of Practice that provides practical guidance on how authorized institutions designated as critical infrastructure operators can comply with the obligations pursuant to PCICSO.[5]

IV. Conclusion

As frontier AI models continue to develop exponentially, we expect AI-enabled cyber resilience to remain an area of close supervisory focus. Senior management (including the Manager-in-Charge of Information Technology in licensed firms) bears ultimate responsibility for managing cybersecurity risks and should ensure that internal policies and procedures are adequately reviewed, enhanced, and approved to align with the SFC and HKMA Circulars. Where appropriate, licensed firms and authorized institutions should also seek independent professional advice and support from information technology specialists.

[1] "*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*", published by the Securities and Futures Commission on June 2, 2026, available here.

[2] "*Strengthening Cyber Resilience amid Artificial Intelligence-Empowered Cyber Threats*", published by the Hong Kong Monetary Authority on June 2, 2026, available here.

[3] "*Appendix: Examples of controls and procedures to manage and mitigate potential risks associated with AI-enabled cyberattacks*", published by the Securities and Futures Commission on June 2, 2026, available here.

[4] Protection of Critical Infrastructures (Computer Systems) Ordinance (Cap. 653), available here.

[5] "*Code of Practice Pursuant to the Protection of Critical Infrastructures (Computer Systems) Ordinance (for Authorized Institutions designated by the Monetary Authority as Critical*

Infrastructure Operators)", published by the Hong Kong Monetary Authority on June 2, 2026, available here.

The following Gibson Dunn lawyers prepared this update: William Hallatt, Becky Chung, and Jane Lu.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. If you wish to discuss any of the matters set out above, please contact any member of Gibson Dunn's Financial Regulatory team, including the following members in Hong Kong:

William R. Hallatt (+852 2214 3836, whallatt@gibsondunn.com)

Emily Rumble (+852 2214 3839, erumble@gibsondunn.com)

Arnold Pun (+852 2214 3838, apun@gibsondunn.com)

Becky Chung (+852 2214 3837, bchung@gibsondunn.com)

Jane Lu (+852 2214 3735, jlu@gibsondunn.com)