Davis Polk

Hong Kong SFC calls for enhanced cybersecurity measures to combat AI-enabled cyberattacks

June 11, 2026 | Client Update | 4-minute read

On June 2, 2026, the Hong Kong Securities and Futures Commission issued a circular urging licensed corporations, virtual asset service providers and associated entities to review and enhance their cybersecurity frameworks to address emerging AI-enabled cyberattacks.

Preparedness for evolving AI threats

Against the backdrop of a 27% year-on-year increase in cybersecurity incidents and the emergence of increasingly sophisticated AI-enabled cyber threats, the circular calls on licensed firms to assess their preparedness for AI-enabled cyberattacks and provides practical guidance to firms on addressing existing vulnerabilities and enhancing cybersecurity controls.

The circular reflects the Securities and Futures Commission's (SFC) engagement with licensed firms and key internet trading platform providers on their preparedness for cyber threats that are increasingly assisted or accelerated by frontier artificial intelligence (AI) models. The circular highlighted two ways in which AI models are amplifying cybersecurity risks:

- **Increased sophistication and frequency of cyberattack:** Frontier AI models possess unprecedented abilities to autonomously identify (i) previously undetected software security flaws, i.e., "zero-day vulnerabilities" and (ii) multiple "lower risk-rated" vulnerabilities (which individually cause minimal impact), which could be chained together and exploited in ways that result in high-impact disruptions. AI-enabled tools also significantly lower the technical barrier for malicious actors to execute phishing, social engineering, deepfake impersonation and reconnaissance.

- **Reduced response time for remedial action:** The availability of low-cost AI tools enables threat actors to rapidly discover and exploit new vulnerabilities, rapidly diminishing the time between identification of a vulnerability and its exploitation. Traditional multi-step patching and change management processes must be expedited to minimize the window of exposure during attacks.

Senior management and MIC-IT accountability

The circular stressed that senior management of licensed firms remains ultimately responsible for managing cybersecurity risks faced by their firms. The SFC explicitly highlighted the role of Manager-in-Charge of Information Technology (MIC-IT) in ensuring adequate review and approval of any changes to their firm's cybersecurity framework and proper and prompt implementation of enhanced cybersecurity measures to address AI risks. Licensed firms are further instructed to seek advice and assistance from external IT security experts as necessary.

Enhanced cybersecurity controls

The circular is accompanied by an Appendix identifying examples of controls and procedures under five key areas that licensed firms are expected to review and consider, namely:

1. Patching and Vulnerability Management

2. Access and Privilege Controls

3. Detection and Monitoring Measures

4. Third-Party Supply Chain Risk Management

5. Incident Response and Recovery

While licensed firms are generally expected to consider the identified measures based on the nature, scale and complexity of their firms' operations and the cybersecurity risks to which they are exposed, certain categories of licensed firms, namely (1) licensed corporations engaged in electronic trading, particularly large retail brokers, (2) depositaries of SFC-authorized collective investment schemes (Type 13 licensed firms) and (3) virtual asset trading platforms (VATPs), are expected to implement all of the controls set out in the circular's Appendix.

Licensed firms' own adoption of AI

The SFC also reiterated its message from the 12 November 2024 Circular on the Use of Generative AI Language Models , that a licensed firm's own deployment of AI language models—whether developed internally, provided by a group affiliate, a third-party service provider or sourced from an open-source model—may amplify existing cybersecurity vulnerabilities and introduce additional risk.

Licensed firms adopting generative AI language models are reminded that (1) AI-specific cybersecurity risks should be addressed within firms' broader cybersecurity frameworks and incident response frameworks, in line with the core principles set out in the November 2024 circular, and (2) where AI language models are used in high-risk use cases (e.g., to provide investment recommendations, investment advice or investment research to clients), the usage is subject to notification requirements under the Securities and Futures (Licensing and Registration) (Information) Rules.

Key takeaways

Given the SFC's indication that it will continue to monitor developments in this area and may conduct reviews to assess firms' preparedness, all licensed firms (especially firms expected to implement all of the controls identified in the circular) should take immediate, proactive steps to align their operations with SFC expectations.

Licensed firms should initiate a cybersecurity framework review, including a gap analysis of existing controls and incident response procedures against the five core areas identified in the circular, to identify any material gaps requiring remediation.

For most financial institutions, given the global nature of the internet, any AI cybersecurity policy needs to be global and calibrated to the regulatory requirements across different markets. Financial regulators across various jurisdictions have expressed concerns about AI-powered cyber threats and many have promulgated regulations and guidance on enhancing cybersecurity. While the underlying requirements are inherently similar, jurisdictions vary in their approach to AI regulation, with some adopting mandatory AI rules and regulations, and others relying on principles-based guidance frameworks.

Jurisdiction	Latest regulatory guidance
US	U.S. Department of the Treasury's Report on Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector New York State Department of Financial Services' Industry Letter re Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks
UK	The Financial Conduct Authority, Bank of England and HM Treasury's joint statement on 15 May 2026 urging financial institutions to take active steps to guard against AI cybersecurity risks
EU	The EU Artificial Intelligence Act
Singapore	Monetary Authority of Singapore's Information Paper on Cyber Risks Associated with Generative Artificial Intelligence (GenAI) Monetary Authority of Singapore's Information Paper on Cyber Risks Associated with Deepfakes Monetary Authority of Singapore's Consultation Paper on Guidelines for Artificial Intelligence Risk Management
Australia	The Australian Securities & Investments Commission issued an open letter on 8 May 2026 to regulated entities urging them to proactively assess and bolster cybersecurity systems

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Martin Rogers
+852 2533 3307
martin.rogers@davispolk.com

Yuan Zheng
+852 2533 1007
yuan.zheng@davispolk.com

Eleanor Tang
+852 2533 1066
eleanor.tang@davispolk.com

Lok Cheung
+852 2533 1029
lok.cheung@davispolk.com

Allison Lau
+852 2533 1016
allison.lau@davispolk.com

Vivien Li
+852 2533 1037
vivien.li@davispolk.com

Katy Choi
+852 2533 1070
katy.choi@davispolk.com

Leanne Chu
+852 2533 3337
leanne.chu@davispolk.com

Caroline Wang
+852 2533 1039
zhuxin.wang@davispolk.com

David Lau
+852 2533 1011
david.lau@davispolk.com