Helpful Guidance on Managing AI-Related Cybersecurity Risks from Hong Kong's SFC

November 19, 2024

On November 12, 2024, Hong Kong's Security and Futures Commission (the "SFC") issued a Circular (the "Circular") with an accompanying appendix (the "Appendix") setting out the SFC's view of the risks associated with the use of generative artificial intelligence language models ("AI LMs") and its expectations for how licensed corporations ("LCs") (generally securities and futures markets participants such as private equity firms, asset managers, or hedge funds that are licensed by the SFC to carry out regulated activities) should be managing and mitigating those risks. Due to the clear and practical guidance offered by the Circular, we suspect it will be influential in how other financial regulators address AI-related risks, and it therefore can serve as a valuable AI risk assessment framework for financial firms that are not LCs.

The Circular, which is effective immediately, is the latest in a growing body of regulatory guidance on generative AI. Some of the issues addressed will be familiar to those who have read the NYDFS's guidance on assessing cybersecurity risks associated with the use of AI. There is also some overlap with the requirements in the EU AI Act and the Colorado AI Law, although the Circular is narrower (applying only to language models) and more prescriptive. The SFC's Circular also comes only a few months after the Hong Kong Monetary Authority issued its own circular on the use of generative AI, indicating a growing interest in the issue by Hong Kong financial regulators.

The Circular offers insight as to how the SFC sees the application of existing regulations (e.g., the Management, Supervision, and Internal Control Guidelines and the Code of Conduct) to AI LM technology. It addresses both AI-related cybersecurity risks, which we cover in this blog post, and other AI governance and operational risks, which we will cover in an upcoming post.

Scope of the Circular

The Circular applies to any SFC LCs "offering services or functionality provided by AI LMs, or AI LM-based third-party products in relation to their regulated activities," which include: dealing in securities or futures contracts; leveraged foreign exchange

trading; advising on securities, futures contracts, or corporate finance; providing automated trading services; securities margin financing; asset management; providing credit rating services; dealing in over-the-counter ("OTC") derivative products or advising on OTC derivative products; providing client clearing services for such OTC transactions; and providing depository services for any relevant collective investment schemes. In the case of virtual asset trading platform providers, regulated activities also include "relevant activities," such as providing services "through means of electronic facilities" and any "off-platform virtual asset trading activities."

The SFC is clear that the requirements outlined in the Circular are intended to reflect a risk-based approach to AI LMs and should be implemented "commensurate with the materiality of the impact and the level of risk presented by the specific use case or application of the AI LM." While the SFC does not provide an exhaustive list of what it deems "high risk," the Circular states that "[g]enerally speaking the SFC considers using an AI LM for providing investment recommendations, investment advice, or investment research to investors or clients as high-risk use cases" for which extra risk mitigation measures should be adopted, as we will discuss in an upcoming Part II of this post.

Cybersecurity Risks for AI

In the Circular and Appendix, the SFC lays out categories of cybersecurity-related risks associated with AI LMs: (1) external threats and internal data privacy and confidentiality risks for LCs' networks; and (2) cyber and operational risks posed by third-party service providers.

Cybersecurity and Data Loss Threats to LCs' Networks

The Circular sets forth the following obligations for protecting LCs' networks from risks associated with AI LMs:

- **Keeping Current**: LCs should keep abreast of the current and emerging cybersecurity threat landscapes and have effective policies, procedures, and internal controls in place to manage the associated cybersecurity risks, including measures to promptly identify cybersecurity intrusions and, where appropriate, suspend the use of an AI LM.

- **Adversarial Testing**: To the extent practicable, LCs should periodically conduct adversarial testing on AI LMs, as well as on any data source system used to train or fine-tune them, to harden and protect them against adversarial attacks.

- **Encryption**: LCs should encrypt non-public data at rest and in transit to ensure their confidentiality and security.

- **Browser Controls**: Because AI LM-based browser extensions may entail privacy and data leakage risks, LCs should mitigate those risks as appropriate, especially if staff have ready access to browser extensions.

- **Sensitive Inputs**: LCs should have controls to assess and mitigate the risks of sensitive confidential information, such as personal data, being input by users or fed into AI LMs.

- **Client Data**: LCs should ensure that controls in relation to confidential client and business information remain effective throughout the model lifecycle.

Third-Party Provider Cyber & Operational Risk

The Circular sets forth the following obligations for protecting LCs from AI-related cybersecurity risks associated with use of AI LMs by third-party providers ("Providers"):

- **Vendor Diligence**: An LC should exercise due skill, care, and diligence in its selection of a Provider, including performing appropriate due diligence and ongoing monitoring to assess whether the Provider possesses the requisite skills, expertise, resources, and controls to deliver the product or service to standards acceptable to the LC.

- **Indemnities**: LCs should assess if a breach by a Provider of applicable personal data privacy or intellectual property laws could have a material adverse impact on them or their use cases, and whether their Providers have measures in place to protect or indemnify the LCs against legal actions or claims against the LCs.

- **Cyber Risk Allocation**: LCs using AI LMs from Providers should ensure that the allocation of responsibilities between them and the Providers in relation to managing cybersecurity risks is well-defined and clearly understood.

- **Supply Chain Risks**: Where an LC's development and deployment of a Provider's AI LM is undertaken with the use of the Provider's data or software, the LC should assess supply chain vulnerabilities as well as data leakage risk at each component of the LC's AI LM architecture and apply stringent cybersecurity controls. An inventory of the Provider's software should be maintained for cybersecurity monitoring.

- **Business Continuity Risks:** LCs using Providers' AI LMs should assess their level of dependence on the consistent delivery and availability of services by those Providers, as well as the potential operational impact on them and their clients if the services are disrupted. LCs should establish appropriate contingency plans to ensure their operational resilience, particularly in relation to critical operations, if the use of any AI LM is disrupted or suspended.

Practical Takeaways

Gap Assessment. LCs should consider conducting a risk assessment that identifies gaps between the requirements in the Circular and their own cybersecurity programs and building a road map for closing any material gaps. For some firms, it may take significant time and resources to fully implement these new requirements, and so they may want to start early. Even firms that are not subject to the Circular may consider conducting a gap analysis in anticipation that similar rules are likely to be adopted by other regulators and may be considered best practices for governance of AI LM-related cybersecurity risks.

Budget. For some firms, compliance with the Circular will require a significant increase in their cybersecurity compliance budgets and the securing of additional resources for 2025 and beyond. Some companies may want to address this now as 2025 budgets are being finalized.

Assessing Significant AI Tools, Vendors, and Use Cases for Cybersecurity Risks. There is no single optimal process for assessing AI-related cybersecurity risk. This can be done as the AI component of a general cybersecurity risk management program or the cybersecurity part of a general AI risk management program. It can also be achieved as the AI and cybersecurity components of more general software and vendor risk management programs. When leveraging their existing resources, controls, and risk management functions, firms will have to decide on the best way to ensure that AI-related cybersecurity risks have been adequately identified and addressed. That process will likely involve some experimentation and pilot programs.

AI Governance Committees Membership. One way to ensure that cybersecurity risks for AI projects are properly addressed is to have a cross-functional committee, with a cybersecurity representative, that approves AI use cases and tools and also assists in the design of AI pilot programs.

Creating Model Diligence Questions and Contract Terms for AI Vendors. AI vendor diligence is a complicated process. Creating model diligence questions and contract

terms will help standardize AI third-party risk management, but companies will still need to determine:

- which kinds of AI vendors are covered (*e.g.*, does the program apply to vendors who leverage AI on their own systems to provide goods and services to the company?);
- what counts as AI (*e.g.*, does it apply to complex algorithms that do not involve machine learning but make important decisions or otherwise present significant reputational or regulatory risk?);
- how much of the program can be standardized (*e.g.*, can diligence and contract terms for risks associated with IP and confidentiality apply to all AI vendors, while risks like bias or antitrust would only be addressed for certain vendors?); and
- which risks are addressed through vendor risk management, and which are addressed separately through the internal use case approval process.

Monitoring AI Use Cases in Production for Scope Creep. For AI use cases that have been approved subject to certain limitations (*e.g.*, no use of confidential data, only one approved AI tool can be used), it is important to periodically check that the actual use is consistent with those limitations and that unanticipated cybersecurity (and other risks) have not materialized.

* * *

The authors would like to thank Debevoise Law Clerks Diane Bernabei and Adam Shankman for their contribution to this blog post.

To subscribe to the Data Blog, please click here.

The Debevoise Data Portal is an online suite of tools that help our clients quickly assess their federal, state, and international breach notification and substantive cybersecurity obligations. Please contact us at dataportal@debevoise.com for more information.

The cover art used in this blog post was generated by DALL-E.

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Gareth Hughes
Partner, Hong Kong
+852 2160 9808
ghughes@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Emily Lam
International Counsel, Hong Kong
+852 2160 9823
elam@debevoise.com

Suchita Mandavilli Brundage
Associate, New York
+1 212 909 6486
smbrundage@debevoise.com