Examples of controls and procedures to manage and mitigate potential risks associated with AI-enabled cyberattacks

This Appendix sets out examples of controls and procedures to help licensed firms review and enhance their cybersecurity framework and manage and mitigate potential risks associated with AI-enabled cyberattacks. These examples are illustrative and not intended to be exhaustive.

LCs engaged in electronic trading, particularly large retail brokers, depositaries of SFC-authorised collective investment schemes (LCs licensed for Type 13 regulated activity) and VATPs are generally expected to implement all of the following measures to better protect themselves against AI-enabled cyberattacks and safeguard their clients' interests and assets. Other licensed firms should consider these measures, taking into account the nature, scale, and complexity of their operations, their technology dependencies, and the cybersecurity risks to which they are exposed.

(A) Patching and vulnerability management

Licensed firms may consider implementing the following patching and vulnerability management procedures:

(a) *Addressing known vulnerabilities*: Accelerate the remediation of existing known vulnerabilities, such as decommissioning legacy systems, replacing end-of-life and unsupported software and deploying released patches in a timely manner, to strengthen overall system security.

Licensed firms are reminded that accumulated unremediated vulnerabilities may represent heightened operational risk where threat actors are able to use AI-enabled tools to accelerate vulnerability analysis, exploit development or attack planning. Firms should therefore critically assess whether current remediation timelines, risk tolerance levels, or patch deferral practices remain appropriate. They should also take steps to minimise unresolved vulnerabilities where practicable, particularly for externally facing and business-critical systems;

(b) *Prioritising patching*: Prioritise patching work by adopting a risk-based approach to ensure that resources are allocated efficiently to address the riskiest vulnerabilities first. This involves evaluating and ranking vulnerabilities based on the severity of the threat, the likelihood of exploitability, the level of external exposure of the system, the sensitivity of the data involved, and the criticality of the affected system to the firm's operations, among other things;

(c) *Automating patching activities*: Automate the patch deployment process where appropriate and feasible to automatically identify patch updates across all servers, networks and systems and validate and implement fixes for "lower risk-rated" vulnerabilities so as to accelerate the deployment of security patches; and

(d) *Implementing compensating measures*: Implement appropriate compensating controls during the patch deployment cycle to reduce exposure until permanent fixes are deployed. For example, utilise firewall or web application firewall (WAF)[1], network controls, and other containment strategies to restrict access to affected systems and reduce risk exposure.

(B) Access and privilege controls

Licensed firms may consider the following access controls to minimise unauthorised access to their systems:

(a) implement phishing-resistant multi-factor authentication on administrative, cloud and privileged accounts;

(b) enforce least-privilege and just-in-time access for all critical systems;

(c) tighten cloud configuration and access controls;

(d) reduce attack-surface by hardening (ie, minimising and disabling unnecessary services, accounts and applications); and

(e) secure development and test environments by ensuring that they do not contain unnecessary copies of production data or credentials, and that any such data is appropriately masked and protected.

Licensed firms may consider strengthening perimeter-level controls designed to slow, disrupt or delay attempted intrusions to support timely detection and containment. Such measures may include enhancing WAF capabilities, adopting cloud edge or content delivery network protections for externally exposed services, and deploying network-based controls that can block or rate-limit anomalous traffic patterns associated with automated exploitation. They may also consider the use of segmentation, controlled exposure of services, and other defensive techniques to reduce the likelihood that the compromise of one system spreads to critical systems.

(C) Detection and monitoring measures

Licensed firms may consider implementing the following detection and monitoring measures:

(a) *Scanning of systems, networks and internal code repositories*: Conduct proactive scanning of systems, networks and internal code repositories to identify abnormal behaviour, irregular traffic, potential vulnerabilities and cyberattacks. Take appropriate remedial actions promptly upon the identification of any issue and irregularity;

[1] WAF is a security solution that monitors, filters, and/or blocks internet traffic to and from a web application.

(b) *Reviewing and enhancing anomaly detection rules*: Review and enhance anomaly detection rules on a regular basis to ensure that they are capable of identifying emerging attack patterns;

(c) *Conducting simulated penetration and resilience testing*: Conduct red team exercises to simulate AI-enabled and other cybersecurity attacks on a periodic basis to ensure that the firm's defence mechanisms are capable of detecting and defending such attacks.

Licensed firms with limited internal resources may leverage their existing IT service providers, cloud platform security tools, or managed security service providers to support testing and threat-hunting; and

(d) *Keeping up-to-date with threat intelligence*: Establish ongoing communication with third-party service providers and security advisors, subscribe to threat intelligence feeds and regularly monitor news sources to stay informed of emerging threats, zero-day vulnerabilities, upcoming patches, and product updates. Promptly assess implications of the intelligence and developments on the firm's cybersecurity risk posture and take timely remedial actions as appropriate.

(D) Third-party supply chain risk management

Licensed firms may consider implementing the following procedures to manage risks in the third-party supply chain:

(a) *Conducting adequate initial and ongoing due diligence on third-party service providers:* Evaluate third-party service providers' cybersecurity framework with reference to established information security standards and control frameworks, such as ISO/IEC 27001, the Information Systems Audit and Control Association's COBIT framework and cybersecurity framework issued by the National Institute of Standards and Technology, supplemented with assessments by independent third-party assurance reports as appropriate.

In particular, identify critical and high-risk service providers (ie, higher risk in terms of supply chain attack) and conduct enhanced assessments covering their vulnerability management process, patch deployment capabilities and other measures undertaken to address AI-enabled cyberattacks;

(b) *Assessing concentration risks*: Assess concentration risk arising from reliance on a small number of critical third-party service providers, and put in place contingency plans that address the disruption or suspension of critical services provided by these service providers; and

(c) *Requiring notifications on cybersecurity incidents*: Ensure that contractual arrangements with third-party service providers address the timely notification of security incidents, protocols for vulnerability disclosure, and exit and contingency arrangements.

(E) Incident response and recovery

Licensed firms may consider specifying the following in their cybersecurity incident handling procedures and contingency plans:

(a) the roles and responsibilities for all personnel involved in the incident response process and set out clear escalation protocols to facilitate coordinated efforts across teams, including IT, risk management, compliance, and senior management;

(b) the pre-authorised containment actions that should be immediately implemented, taking into account that AI-enabled cyberattacks may unfold more quickly than traditional detection and escalation processes; the plan should also detail other actions required for the recovery of the firm's operations and maintaining operational continuity, ensuring that these are closely aligned with the firm's recovery time and recovery point objectives; and

(c) the communication strategies with all affected stakeholders, including clients, third-party service providers, law enforcement agencies, and the SFC, as applicable.