October 30, 2024

AI Cybersecurity Guidance Summary - NYDFS and Singapore CSA

by Anthony D. Glosson , Gregory P. Silberman , Jon Neiditz

As regulators worldwide continue to scrutinize the impact of AI on industries within their respective purviews, two key global agencies issued guidance in October 2024 that highlighted AI-based cybersecurity risks and best practices. Specifically, the New York State Department of Financial Services ("DFS") and the Cyber Security Agency of Singapore ("CSA") each released robust guidance documents addressing the cybersecurity challenges posed by artificial intelligence systems. The two regulators approached the subject from a different perspective, but both provided important frameworks for organizations to assess and mitigate AI-related cybersecurity risks. In this client alert, we analyze the key points from both guidance documents and examine their approaches to AI security.

NYDFS Guidance Overview

The NYDFS guidance outlines cybersecurity risks and opportunities that artificial intelligence presents in the financial services sector. While the guidance is specifically applicable to financial services organizations and related platform or service providers doing business in New York, the recommendations set forth therein nevertheless offers key insights that organizations from other sectors and jurisdictions can use to harden their cybersecurity postures relative to AI.

The NYDFS identified AI-enabled social engineering as one of the most significant threats, whereby threat actors create highly convincing deepfake content across various communication channels. These sophisticated attacks have led to unauthorized information disclosure and fraudulent financial transfers, with some incidents resulting in millions in losses.

The guidance highlights how AI has strengthened existing cyberattack capabilities, enabling threat actors to identify vulnerabilities, conduct reconnaissance, and develop malware variants more efficiently than ever before. This enhancement has lowered the technical barrier for conducting cyberattacks, which may increase the frequency and severity of incidents in the financial sector.

For example, the NYDFS recounted how, in February 2024, a finance worker at a multinational company in Hong Kong fell victim to an elaborate scam that used deepfake technology to impersonate senior executives, resulting in a loss of over $25 million. The incident began when the employee received a fake message supposedly from the company's chief financial officer, inviting them to a video call to discuss a confidential transaction. During the call, several participants, appearing as executives of the firm, were actually deepfake

recreations. The deepfake technology used real video footage of the executives, manipulated with artificial intelligence to convincingly imitate their appearances and voices. This created the illusion of a legitimate multi-person meeting, leading the employee to authorize 15 transactions, transferring $25.6 million to five different bank accounts.

Covered organizations are required to conduct regular risk assessments that specifically address AI-related threats, including their own use of AI and technologies utilized by third-party service providers. The guidance mandates multi-factor authentication by November 2025 for all authorized users accessing regulated entities' information systems or nonpublic information. It recommends authentication methods that can withstand deepfake attempts, such as digital certificates and physical security keys, rather than traditional biometric systems alone.

The document emphasizes comprehensive cybersecurity training for all personnel and outlines data management requirements, including data minimization practices and detailed inventory maintenance.

While acknowledging the risks deriving from AI, the guidance also recognizes how AI can significantly benefit cybersecurity efforts through enhanced threat detection, automated routine tasks, and expedited incident response.

Singapore CSA Guidance Overview

The CSA guidance establishes a comprehensive framework for securing AI systems across all economic sectors. The document promotes AI security by design and by default, similar to other software systems. These guidelines, though not mandatory, help system owners manage security risks throughout the AI lifecycle.

The guidance identifies two main threat categories: classical cybersecurity risks (including supply chain attacks and unauthorized access) and novel threats specific to AI, particularly Adversarial Machine Learning attacks. It presents a lifecycle approach to AI security through five key stages: Planning and Design, Development, Deployment, Operations and Maintenance, and End of Life.

The CSA directs organizations to begin with comprehensive risk assessments, followed by systematically prioritizing areas based on risk and impact, implementing security actions, and evaluating residual risks. The guidelines offer detailed recommendations across each lifecycle stage, from awareness-raising during planning to proper disposal of data and models at end-of-life.

A companion guide supplements the main document with practical security control measures, acknowledging AI security's evolving nature. The guidelines stress that no one-size-fits-all solution exists, and organizations must tailor their approach to their specific context and use cases.

Conclusion

The NYDFS and CSA guidance documents share the common goal of promoting secure AI implementation but differ significantly in their approach and scope. The NYDFS takes a more prescriptive approach, linking directly

to existing regulatory requirements for financial institutions, with specific deadlines and mandatory controls. It concentrates heavily on protecting against social engineering attacks and safeguarding financial transactions, reflecting the financial services sector's specific concerns.

The CSA guidance offers a broader, more flexible approach that applies across all industries. It emphasizes the full lifecycle of AI systems and creates a general framework that organizations can adapt to their needs. While the NYDFS guidance focuses on protecting against specific threats, the CSA document takes a more holistic view of AI security, incorporating both traditional cybersecurity concerns and AI-specific challenges.

Both documents emphasize risk assessment, supply chain security, and continuous monitoring, and both offer valuable insights for organizations seeking to address emerging security challenges posed by AI systems, all while acknowledging how the technology can enhance cybersecurity capabilities. Taken together, they demonstrate growing recognition that organizations need structured approaches to manage AI-related security risks across different regulatory contexts and industries.