December 20, 2024

AI Cyber Risk and Mitigation Guidance from the New York State Department of Financial Services

Banks, insurance companies, partnerships, agencies, associations and other entities registered or licensed under the New York State banking, insurance or financial services laws ("Covered Entities") are regulated by the New York State Department of Financial Services ("NYS DFS"). The NYS DFS views its role as establishing certain regulatory minimum standards and providing guidance and resources to assist in these efforts. In that capacity, the NYS DFS has been on the forefront of cybersecurity regulation, initially in 2017 with the Cybersecurity Requirements for Financial Services Companies[1] (the "Cybersecurity Regulation") and most recently in October 2024 with the Industry Letter regarding Cybersecurity Risk Arising from Artificial Intelligence and Strategies to Combat Related Risks (the "AI Cyber Risk Letter").[2]

The AI Cyber Risk Letter provides guidance about how AI use may be assessed and risks mitigated in accordance with the existing Cybersecurity Regulation. As explained at the end of the letter, "[a]s AI continues to evolve, so too will AI-related cybersecurity risks. Detection of, and response to, AI threats will require equally sophisticated countermeasures, which is why it is vital for Covered Entities to review and reevaluate their cybersecurity programs and controls at regular intervals, as *required* by Part 500." (emphasis added).

As summarized below, the AI threat landscape and possible mitigation measures are the main topics of the AI Cyber Risk Letter. On a positive note, the letter also observes that AI capabilities, such as its ability to quickly perform routine tasks and analyze data, may help mitigate risks. In general, for Covered Entities as well as other entities not governed by NYS DFS regulations, the AI Cyber Risk Letter provides a useful framework to proactively assess and manage AI risks.

Threat Landscape

AI-Enabled Social Engineering

Threat actors can leverage AI to create highly personalized and sophisticated content for social engineering, including realistic deepfakes that may convincingly mimic real individuals at little to no cost and without technical expertise. Such feats of social engineering may be more likely to succeed and result in disclosure of sensitive information or actions like wiring money to the threat actor.

AI-Enhanced Cybersecurity Attacks

The power of AI to process and analyze information accelerates the activities of threat actors to penetrate systems and exploit security vulnerabilities. AI also can help threat actors to change malware and ransomware to keep ahead of defensive security controls. Furthermore, according to the AI Cyber Risk Letter, AI lowers the barrier to entry for cybercrimes, so even low skilled threat actors can launch cyberattacks. AI also makes it possible to conduct more attacks more quickly.

Exposure or Theft of Vast Amounts of Nonpublic Information ("NPI")

Covered Entities seeking to deploy AI may maintain or allow access to troves of data. This creates a target-rich environment for threat actors. Data may include personal data, which makes the consequences of a cyberattack more severe and could

implicate various data privacy laws. In addition, some data may include biometric data, such as facial images, or fingerprints that potentially could be used to imitate users to gain access to systems.

Increased Vulnerabilities Due to Third-Party, Vendor, and Other Supply Chain Dependencies

AI often requires coordination with third party service providers, which adds another link in the supply chain that could be exploited by threat actors leading to increased exposure to risk.

Mitigation Measures

To mitigate risks, the AI Cyber Risk Letter recommends considering and implementing the following measures:

- *Multiple Controls:* Multiple or redundant layers of security controls should protect systems (note the similarity to the multi-factor authentication requirement in the Cybersecurity Regulation). For instance, a good practice includes training employees to always ask for verification in a second, different format in order to mitigate the risk that someone might create a deepfake video mimicking a supervisor asking for money to be transferred.
- *Updating Risk Assessments*: AI threats should be covered in required periodic risk assessments, as well as related policies and procedures and information governance programs. According to the AI Cyber Risk letter, "[t]he Cybersecurity Regulation requires Risk Assessments to be updated at least annually and whenever a change in the business or technology causes a material change to a Covered Entity's Information Systems or NPI."
- *Plan Updates and Testing:* Incident response, business continuity and disaster recovery plans could be tested and updated to address emerging AI risks, including identifying systems that rely on AI and are critical for ongoing business operations. Consider conducting AI-focused tabletop exercises.
- *Management Reports and Awareness*: NYS DFS expects management to be aware of and receive reports about emerging cybersecurity risks, including relating to AI.
- *Third Party Risk Management:* NYS DFS "strongly recommends" that Covered Entities add AI threats to their existing approach to due diligence for third parties, especially those with access to information systems or NPI. It is recommended to review and update existing contracts with AI representations and warranties to confirm that the third parties are obligated to provide timely notification of cybersecurity events, including threats related to AI.
- *Access Controls*: NYS DFS reiterates the importance of multifactor authentication and other access controls, as determined by Covered Entities based on their required risk assessments. It is recommended to evaluate the effectiveness of such multifactor authentication and other controls, especially in this era of deepfakes and other AI-enhanced attacks, and to consider using new techniques like biometrics and to layer in additional access controls for systems containing NPI.
- *Updates to Cybersecurity Training*: Training on cybersecurity, including for senior management and third parties, should be updated to raise awareness of AI risks and AI-enabled social engineering. Such training ideally will emphasize the need for redundancy in verification methods to address deepfakes, as discussed above.
- *Monitoring:* In addition to their existing obligations to monitor systems containing NPI for security vulnerabilities, Covered Entities that permit personnel to use generative AI tools, such as ChatGPT, are advised by the NYS DFS to "consider monitoring for unusual query behaviors that might indicate an attempt to extract NPI and blocking queries from personnel that might expose NPI to a public AI product or system."
- *Data Management:* Reducing storage of data, especially NPI, reduces the risk of exposure. By November 1, 2025, Covered Entities will be required to maintain and update data inventories, which will help to assess risks and to pinpoint what NPI or systems are impacted if a breach occurs. The NYS DFS's guidance is that "[e]ntities should implement data governance procedures that include data collection, storage, processing, and disposal." Such data inventories and governance should specify which systems use or rely on AI.

If you have questions or seek advice related to the topic of this article, please feel free to contact one of the Day Pitney lawyers listed above.

[1] 23 NYCRR pt. 500.

[2] Industry letter from New York State Department of Financial Services (DFS) to the executives and information security personnel at all entities regulated by the DFS (Oct. 16, 2024).

Authors

Laura Land Himelstein
Counsel

New York, NY | (212) 297-2471

lhimelstein@daypitney.com

Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com

William J. Roberts
Partner

Hartford, CT | (860) 275-0184

wroberts@daypitney.com

Ashley Picker Dubin

Counsel

Hartford, CT | (860) 275-0155

adubin@daypitney.com