Alert

October 24, 2024

COZEN O'CONNOR

NYDFS Issues Guidance on Cybersecurity Risks Arising from Artificial Intelligence

On October 16, 2024, the New York Department of Financial Services (NYDFS) issued an Industry Letter that discusses the cybersecurity risks associated with the use of artificial intelligence (AI) and outlines strategies to manage these risks. The Industry Letter, which only applies to those entities regulated by the NYDFS (Covered Entities), does not introduce any additional requirements beyond those outlined in 23 NYCRR Part 500 (the NYDFS Cybersecurity Regulation). However, the Industry Letter aims to describe how Covered Entities should utilize the compliance framework within the NYDFS Cybersecurity Regulation to evaluate and mitigate the cybersecurity risks arising from AI and, therefore, provides a roadmap of issues the NYDFS might focus on in enforcement proceedings.

Risks Arising from the Use of AI

The Industry Letter highlights several of the most significant cybersecurity risks related to AI. It focuses on risks caused by a threat actor's use of AI and risks caused by a Covered Entity's use of or reliance upon AI.

The NYDFS cautions that threat actors are leveraging AI to produce convincing deepfakes, targeting individuals via email, phone, video calls, and online posts. These AI-powered attacks frequently attempt to trick employees into revealing sensitive personal and company information. When deepfakes lead to the sharing of company credentials, threat actors are often able to gain access to information systems containing nonpublic information.

The NYDFS also warns that threat actors can use AI to enhance the potency, scale, and speed of traditional cyberattacks. By leveraging AI's ability to quickly scan and analyze vast amounts of data, threat actors can more rapidly discover and exploit security vulnerabilities, allowing them to breach information systems at a quicker pace.

The NYDFS also notes that threat actors lacking the prior technical expertise to perform cyberattacks may now be capable of conducting their own cyberattacks using AI. The NYDFS believes that this development could lead to a rise in both the frequency and severity of cyberattacks, particularly in the financial services industry, where the maintenance of highly sensitive nonpublic information creates an attractive target for threat actors.

Finally, the NYDS highlights that supply chain vulnerabilities are a critical concern for organizations using AI. AI-powered tools rely on data collection and maintenance, which often involves working with vendors and third-party service providers. Each link in this supply chain can introduce security risks exploitable by threat actors, potentially exposing an entity's nonpublic information and leading to broader attacks on the entire network.

Recommended Controls and Measures that Mitigate AI-Related Risks

In the Industry Letter, the NYDFS recommends that Covered Entities implement comprehensive controls and measures to mitigate against these AI-related risks. The NYDFS emphasizes that when Covered Entities design risk assessments and cybersecurity programs, as required by the NYDFS Cybersecurity Regulation, these assessments and programs must now consider risks associated with deepfakes and other threats posed by AI in the hands of external actors. The NYDFS also recommends that Covered Entities should address AI-related risks stemming from their own use of AI, AI used by their third-party service providers and vendors, and the potential vulnerabilities in AI applications (e.g., ChatGPT).

The Industry Letter emphasizes the importance of implementing policies and procedures that

Andrew Baer

Chair, Technology, Privacy & Data Security

abaer@cozen.com
Phone: (215) 665-2185
Fax: (215) 372-2400

Robert W. Rubenstein

Associate

rrubenstein@cozen.com
Phone: (215) 366-4472
Fax: (215) 665-2013

Related Practice Areas

- Business
- Corporate
- Technology, Privacy & Data Security

outline guidelines for performing due diligence on AI-powered third-power service providers before a Covered Entity engages its services. When a Covered Entity engages a third-party service provider that utilizes AI, the NYDFS recommends including additional representations and warranties in the agreements with the third-party service provider related to the secure use of the Covered Entities' nonpublic information, including requirements to take advantage of available enhanced privacy, security, and confidentiality options.

The Industry Letter also underscores the need for Covered Entities to implement robust access controls to combat AI-related risks. The NYDFS mentions that multi-factor authentication is one of the most effective access controls, which the NYDFS Cybersecurity Regulation already requires. In light of the heightened risks associated with using AI, the NYDFS suggests that Covered Entities adopt authentication factors that can withstand AI-manipulated deepfakes and other AI-enhanced attacks. For example, the NYDFS recommends avoiding authentication via SMS text, voice, or video and using forms of authentication that AI deepfakes cannot impersonate, such as digital-based certificates and physical security keys.

Furthermore, while the NYDFS Cybersecurity Regulation has always required cybersecurity training for Covered Entity personnel, the Industry Letter recommends that cybersecurity trainings should now be updated to include AI-related risks. Trainings should cover how threat actors are using AI in social engineering and deepfake attacks, how AI is being used to facilitate and enhance existing types of cyberattacks, and how AI can be used to improve cybersecurity.

With respect to the NYDFS Cybersecurity Regulation's requirement for Covered Entities to have a monitoring process in place that is capable of identifying new security vulnerabilities, the NYDFS recommends that those Covered Entities using AI-enabled products or services or permitting personnel to use AI applications (like ChatGPT), should consider monitoring for unusual query behaviors indicative of attempts to extract nonpublic information.

In relation to the NYDFS Cybersecurity Regulation's requirement for Covered Entities to adopt data minimization practices, the NYDFS mentions that Covered Entities must dispose of nonpublic information that is no longer necessary for business operations or other legitimate business purposes, including nonpublic information used for AI purposes.

Lastly, starting November 1, 2025, the NYDFS Cybersecurity Regulation will require Covered Entities to maintain and update data inventories. The NYDFS recommends that Covered Entities also begin keeping an inventory of all information security systems that utilize or rely on AI-enabled products and services.

Conclusion

While the NYDFS points out various AI-related risks in the Industry Letter, it also recommends that Covered Entities explore the considerable cybersecurity advantages that can come from incorporating AI into their security tools, controls, and strategies. The NYDFS acknowledges that AI's ability to quickly and accurately analyze vast amounts of data can be valuable for developing a cybersecurity program and implementing cybersecurity controls. The release of this Industry Letter suggests that the NYDFS is monitoring the growing use of AI and its associated risks, which may signal the NYDFS' future enforcement priorities.