# Cybersecurity Risks Arising from AI and Strategies to Combat those Risks

**October 19, 2024**

**By Mel Tull**

The New York Department of Financial Services (DFS) recently issued guidance addressing the cybersecurity risks associated with artificial intelligence (AI) and strategies to combat those risks.[1] Even if you do not do business in New York, this guidance is informative for insurance agents to understand how AI impacts cybersecurity and what strategies can be employed to mitigate these risks. Here's what insurance agents need to know about the guidance and how to prepare for these evolving threats.

## Background

The guidance does not impose any new requirements beyond obligations that are in the NYDFS's existing cybersecurity regulations.[2] Rather, the guidance is meant to explain how covered entities should use the framework required by the existing NYDFS cybersecurity regulations to assess and address the cybersecurity risks arising from AI. Virginia insurance agencies are subject to a similar framework in the Virginia Insurance Data Security Act,[3] and the NYDFS guidance is instructive for agencies complying with the Virginia Act.

Advancements in AI have significantly transformed the cybersecurity landscape. While AI introduces new opportunities for cybercriminals to exploit vulnerabilities at a greater scale and speed, it also offers substantial benefits in enhancing threat detection and incident response. The NYDFS guidance aims to help regulated entities, including insurance agencies, understand and address AI-related cybersecurity risks.

## Key Cybersecurity Risks Associated with AI

### AI-Enabled Social Engineering

AI has enhanced the sophistication of social engineering attacks. Cybercriminals use AI to create highly personalized and convincing content, such as deepfakes, to deceive individuals into divulging sensitive information. These attacks can occur through various channels, including email (phishing), telephone (vishing), text (SMiShing), and online postings. The realistic nature of AI-generated content makes it more challenging to detect and prevent these attacks.

### AI-Enhanced Cybersecurity Attacks

[1] New York Department of Financial Services, Industry Letter, Re: Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks, October 16, 2024.

[2] 23 NYCRR Part 500.

[3] Code of Virginia, Title 38.2, Chapter 6, Article 2. Insurance Data Security Act.

AI enables cybercriminals to amplify the potency, scale, and speed of cyberattacks. By leveraging AI, threat actors can quickly identify and exploit security vulnerabilities, conduct reconnaissance, and deploy malware more effectively. AI also facilitates the development of new malware variants and the evasion of defensive security controls, increasing the severity and frequency of cyberattacks.

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

AI systems often require large amounts of data, including NPI, for training and operation. This increases the risk of data breaches, as cybercriminals target these data-rich environments to extract valuable information. Additionally, the use of biometric data in AI applications poses further risks, as stolen biometric data can be used to bypass authentication mechanisms and create realistic deepfakes.

### Increased Vulnerabilities Due to Third-Party Dependencies

AI-powered tools and applications rely heavily on data from third-party vendors and service providers. Each link in this supply chain introduces potential security vulnerabilities. A cybersecurity incident affecting any third-party provider can expose an entity’s NPI and create a gateway for broader attacks on the entity’s network.

## Strategies to Mitigate AI-Related Cybersecurity Risks

The NYDFS guidance outlines several strategies that insurance agencies can implement to mitigate AI-related cybersecurity risks. These strategies align with the requirements of the NYDFS Cybersecurity Regulation (23 NYCRR Part 500).

### Risk Assessments and Risk-Based Programs

Insurance agencies should conduct comprehensive risk assessments to identify and evaluate AI-related cybersecurity risks. These assessments should inform the development of risk-based cybersecurity programs, policies, and procedures tailored to address the specific threats posed by AI.

### Enhanced Security Controls

Implementing multiple layers of security controls can provide overlapping protections against AI-related threats. Key controls include:

- **Multi-Factor Authentication (MFA):** Strengthening authentication mechanisms to prevent unauthorized access.
- **Encryption:** Protecting sensitive data both in transit and at rest.

- **Network Segmentation:** Isolating critical systems and data to limit the impact of a breach.
- **Continuous Monitoring:** Using AI-driven tools to detect and respond to anomalies in real-time.

### Employee Training and Awareness

Educating employees about the risks associated with AI and social engineering attacks is crucial. Regular training sessions can help employees recognize and respond to phishing attempts, deepfakes, and other AI-enabled threats.

### Vendor Management

Insurance agencies should implement robust vendor management practices to ensure that third-party providers adhere to stringent cybersecurity standards. This includes conducting due diligence, regular audits, and requiring vendors to comply with the agency's cybersecurity policies.

### Use AI to Your Advantage to Mitigate Cybersecurity Risks

On the positive side, the NYDFS guidance encourages organizations to explore the substantial cybersecurity benefits that can be gained by integrating AI into cybersecurity tools, controls, and strategies. AI's ability to analyze vast amounts of data quickly and accurately is tremendously valuable for: automating routine repetitive tasks, such as reviewing security logs and alerts, analyzing behavior, detecting anomalies, and predicting potential security threats; efficiently identifying assets, vulnerabilities, and threats; responding quickly once a threat is detected; and expediting recovery of normal operations.

## What Should Insurance Agencies Do Now?

To prepare for the evolving cybersecurity landscape, insurance agencies should take the following steps:

1. **Conduct Risk Assessments:** Evaluate the cybersecurity risks associated with AI and update risk management strategies accordingly.
2. **Enhance Security Controls:** Implement and regularly update security controls to protect against AI-related threats.
3. **Train Employees:** Provide ongoing training to employees on recognizing and mitigating AI-enabled cyber threats.
4. **Manage Vendors:** Ensure that third-party vendors comply with cybersecurity standards and conduct regular assessments of their security practices.
5. **Stay Informed:** Keep abreast of the latest developments in AI and cybersecurity to adapt strategies as needed.

**Conclusion**

The NYDFS guidance on AI-related cybersecurity risks underscores the importance of proactive measures to protect sensitive information and maintain robust cybersecurity defenses. By understanding the risks and implementing the recommended strategies, insurance agencies can better safeguard their operations and clients against the evolving threats posed by AI.

For more information or assistance with developing policies and procedures for protecting against cybersecurity risks and complying with cybersecurity regulations, contact Mel Tull, at Mel@TullLawPLC.com or (804) 404-7748. Mel advises insurance agencies and other companies on general business law matters, regulatory compliance issues, and buying and selling businesses, agencies and books of business.

*This article has been prepared for informational purposes only and is not legal advice.*