PUBLICATION

New York DFS Releases AI Cybersecurity Guidance

Authors: Aldo M. Leiva, Matthew George White
October 22, 2024

The New York Department of Financial Services (NYDFS) issued new guidance (the Guidance) on October 16, 2024, to help state-regulated financial institutions mitigate the myriads of cybersecurity risks posed by artificial intelligence (AI). While the Guidance does not impose new requirements, it provides an outline for regulated entities to use in meeting existing compliance obligations under the NYDFS Cybersecurity Regulation (23 NYCRR Part 500). The Guidance outlines measures to protect against several AI-specific risks:

1. **AI-Enabled Social Engineering**: AI has improved and expanded the ability of threat actors to create highly personalized and more sophisticated content that is more likely to be convincing than historical social engineering attempts (*think*: the foreign prince who just needs $100 to unlock his treasure chest). These AI-driven attacks often attempt to convince individuals and employees to divulge sensitive information about themselves, their families, and their employers. Many of these so-called "Deepfakes" pose significant financial and operational threats to companies. See our prior analysis of Deepfakes, available here.

2. **AI-Enhanced Cybersecurity Attacks**: AI can scan and analyze vast amounts of information much faster than humans, allowing threat actors to quickly identify and exploit security vulnerabilities. AI can also accelerate the development of new malware variants and changed ransomware to enable it to bypass defensive security controls. Indeed, AI-powered tools can be used to obfuscate a variety of malicious cyber activities, making it more difficult for traditional security systems to detect and respond to threats in a timely manner. This means, AI in the hands of hackers can be like a GPS for burglars, instantly mapping out the weakest points of entry and rerouting around any new security obstacles with ease.

3. **Exposure or Theft of Vast Amounts of Nonpublic Information (NPI)**: AI-driven products frequently require the collection and analysis of vast amounts of data to function effectively, which often includes NPI. This data is critical for training AI models and improving their accuracy, but its collection raises significant privacy and security concerns as the more sensitive data an organization holds, the higher the potential risk of breaches or misuse. Maintaining NPI in large quantities poses additional risks for entities that develop or deploy AI. Storing vast amounts of sensitive data for AI use is like stockpiling fuel for a powerful engine – but the more fuel you store, the greater the risk of a devastating fire if safeguards aren't airtight.

4. **Increased Vulnerabilities Due to Third-Party, Vendor, and Other Supply Chain Dependencies**: AI-powered tools and applications depend heavily on the collection and maintenance of vast amounts of data, often involving working with vendors and Third-Party Service Providers (TPSPs) for data collection, storage, and processing. Each link in this supply chain introduces potential security vulnerabilities and may be an additional entry point for cybercriminals. Even if an organization maintains strong internal security practices, the weakest link in this chain – whether a poorly secured vendor system or an overlooked vulnerability in a TPSP – can expose the entire network to risks like data breaches, malware, or unauthorized access. Remember: in an AI-driven world, every third-party connection is a potential doorway – one weak lock, and the whole system is at risk.

According to the Guidance, regulated entities should consider and pursue the following action items to protect against these AI cybersecurity risks:

1. **Risk Assessments and Risk-Based Programs, Policies, Procedures, and Plans**: Entities should maintain cybersecurity programs, policies, and procedures based on cybersecurity risk assessments. These assessments should take into account the specific cybersecurity risks likely faced by the entity, including deepfakes, social engineering, and other threats posed by AI.

2. **Continue Assessing Access Controls**: Implementing robust access controls, such as multifactor authentication (MFA) – at all critical access points – is essential to combat attacks generated by deepfakes and other forms of AI-enhanced social engineering. Proper access controls and password management programs can serve as an excellent first line of defense but must be properly designed, maintained, and followed.

3. **Cybersecurity Training**: Training should be provided for all personnel, including senior executives and governing body members. Such training should ensure all personnel are aware of the risks posed by AI and how to identify and respond to AI-enhanced social engineering attacks.

4. **Monitoring**: Entities must have a monitoring process in place to detect unauthorized access to, use of, or tampering with information systems. Monitoring should include the activity of authorized users as well as email and web traffic to block malicious content. Companies might also consider AI-based cybersecurity tools, where appropriate, to buttress their defenses. For our discussion of some of these tools, see here.

5. **Data Management**: Effective data management will limit the NPI at risk of exposure if a threat actor gains access to an entity's information systems. Entities should implement data minimization practices, maintain data inventories, and adhere to an appropriately developed document retention and destruction schedule. Consider: data mapping is your blueprint – without it, your cybersecurity house is built on shaky ground.

In conclusion, NYDFS has made it clear that while AI offers substantial benefits to cybersecurity, it also introduces significant risks that require a proactive approach to manage. The increasing reliance on AI for processing vast amounts of data makes entities vulnerable at multiple points, particularly through third-party relationships and the potential for data misuse. Organizations must implement robust governance frameworks, ensure third-party risk management, and use AI responsibly, keeping both cybersecurity and compliance in mind, along with their evolving regulations. As AI continues to reshape the landscape, vigilance and adaptive strategies will be critical for mitigating risks and ensuring both consumer protection and operational resilience. As these challenges grow more and more complex, legal expertise is essential. Consulting experienced cybersecurity and data privacy attorneys can help you navigate the regulatory landscape, minimize risks, and develop tailored strategies to protect your business. Don't hesitate to reach out to Aldo M. Leiva, Matthew G. White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team for guidance and support.