WINSTON & STRAWN LLP

BLOG

Key Compliance Strategies: NY Department of Financial Services' Guidance on AI and Cybersecurity Threats

OCTOBER 22, 2024

On October 16, 2024, the New York Department of Financial Services (DFS) released an important industry guidance letter aimed at addressing the novel, complex cybersecurity risks associated with artificial intelligence (AI).[1] In it, DFS responds to inquiries from entities subject to DFS regulation, including banks, insurance companies, and financial service providers.[2] The implications of this guidance letter extend beyond New York's borders, serving as a resource for organizations and executives operating in different jurisdictions. The insights offered in this document not only highlight emerging threats but also provide actionable best practices for mitigating these risks.

KEY TAKEAWAYS

- **AI-Driven Threats**: Organizations must recognize the increasing sophistication of AI-enabled social engineering attacks, including deepfakes, which pose significant risks to identity verification and data security.
- **Robust Cybersecurity Programs**: Compliance with the DFS Cybersecurity Regulation requires comprehensive cybersecurity programs based on regular risk assessments, proactive incident response plans, and strong leadership commitment.
- **Third-Party Oversight**: Enhanced due diligence and ongoing monitoring of third-party service providers (TPSPs) are essential to ensure they meet cybersecurity-industry standards and protect sensitive information.
- **Data Governance and Minimization**: Organizations should prioritize data minimization practices, ensuring responsible disposal of nonpublic information (NPI) and implementing robust controls to safeguard data, particularly in AI applications.

THE EVOLVING LANDSCAPE OF CYBER THREATS

DFS's foremost concern is the rise of AI-enabled social engineering attacks. Unlike traditional phishing schemes, modern social engineering threats are highly personalized and sophisticated. Malicious actors employ AI as a trawl to analyze individual social media profiles, online interactions, and other publicly available information to create tailored attacks. This hyper-personalization enables cybercriminals to deceive employees into revealing sensitive data or engaging in harmful activities.

A particularly alarming advancement in this space is the use of deepfake technology—the creation of hyper-realistic audio and video content that can impersonate individuals convincingly. This capability not only complicates identity verification but also opens the door for fraud. The DFS industry letter includes several global examples of deepfake technology fooling powerful companies.[3]

DFS emphasized how AI enhances the speed, scale, and frequency of cyber attacks. Traditional cybercriminals often rely on time-consuming tactics to breach systems, but AI can automate and accelerate these processes. By rapidly identifying vulnerabilities and deploying attacks, AI enables bad actors to orchestrate large-scale campaigns with alarming efficiency.

Another concern is the exposure of NPI. Many organizations implement biometric authentication systems as an extra layer of security. Even so, as highlighted by DFS, these systems are not impervious to AI-driven attacks and may even be their target. Cybercriminals can exploit vulnerabilities in biometric systems, thereby increasing the risk of unauthorized access to sensitive information. As organizations increasingly rely on biometric data, it is imperative to assess and bolster the security of these systems.

Finally, DFS highlights the issue of third-party supply dependencies. In an interconnected world, organizations often rely on TPSPs to support various business functions. While this enhances operational efficiency, it also introduces additional vulnerabilities. The risk of a compromised TPSP can lead to significant repercussions for an organization. As such, DFS urged companies to evaluate access controls, encryption, and due diligence guidelines for their contractors.

STRATEGIES FOR MITIGATING RISK

To address these multifaceted risks, DFS outlines several essential strategies that regulated entities must adopt. First, and crucial for New York businesses, compliance with DFS's Cybersecurity Regulation requires organizations to establish comprehensive cybersecurity programs. Compliance officers must tailor these programs to the "size, business model, and complexity as well as the type of data" the business maintains.[4] The program should incorporate regular risk assessments designed to identify vulnerabilities and enable companies to adjust their strategies in real time.

Proactive measures for investigating and mitigating cybersecurity events are also paramount. Businesses must have defined incident response plans that outline the responsive steps in the event of a breach. This includes establishing communication protocols, identifying key stakeholders, and conducting post-incident reviews to learn from any failures. The involvement of senior leadership is vital in fostering a culture of compliance; when leaders prioritize cybersecurity, it sends a strong message throughout the organization about the importance of protecting sensitive information.

Enhancing third-party oversight practices is another critical component of the DFS guidance letter. DFS urged organizations to implement rigorous due diligence practices before engaging TPSPs. This includes assessing the cybersecurity measures that TPSPs have in place and requiring regular compliance documentation. Furthermore, organizations should conduct periodic audits of their TPSPs to ensure ongoing adherence to cybersecurity standards. By holding TPSPs to the same level of scrutiny it holds itself to, organizations can mitigate the risks associated with outsourcing necessary functions.

Access controls are another focus of the DFS industry letter. N.Y. C.R.R. § 500.12 mandates that by November 2025, all DFS-regulated organizations must implement multifactor authentication (MFA) across all systems. MFA serves as an essential barrier against unauthorized access, requiring users to provide multiple forms of verification before accessing internal systems.

In addition to technical controls, DFS underscores the importance of cybersecurity training for all employees. Annual cybersecurity awareness training has become a requirement, emphasizing that cybersecurity is a collective responsibility within the organization. This training should enable employees and management to recognize social engineering attempts, understand the implications of AI, and promote best practices for data protection.

Monitoring processes play a crucial role in identifying and mitigating security vulnerabilities. This is particularly relevant for organizations that use AI applications as monitoring for anomalies can help identify potential attempts to extract NPI. By proactively addressing these threats, organizations can mitigate potential breaches before they escalate.

Data control practices are equally important in the context of cybersecurity. DFS emphasizes the need for data minimization, urging organizations to dispose of NPI responsibly when it is no longer necessary for business operations. This is especially critical for organizations using AI as AI algorithms require vast amounts of data to function effectively. But without proper controls in place, this data could become a target for cybercriminals. Organizations must ensure that they have robust data governance frameworks to manage and protect sensitive information.

DFS AND DOJ ALIGNMENT

Last month, we discussed how the U.S. Department of Justice (DOJ) revised its Evaluation of Corporate Compliance Programs to focus more on how organizations are incorporating AI into their business and their compliance programs. This alignment between DOJ and DFS expectations signals a broader recognition of the complexities introduced by AI and the need for comprehensive compliance strategies that include an assessment of disruptive technology risks (including AI). For compliance professionals and information security personnel, this means that organizations must adapt their compliance programs accordingly. This involves not only enhancing existing policies but also developing new frameworks that specifically address AI-related risks.

PRACTICAL IMPLICATIONS FOR COMPLIANCE PROGRAMS

DFS's letter provides compliance professionals in New York with essential guidance for navigating the complexities of modern cybersecurity. To effectively implement these strategies, organizations should consider the following practical implications:

- **Conduct Comprehensive Risk Assessments**: Compliance programs should integrate regular and thorough risk assessments that specifically address AI-related threats. This includes evaluating the effectiveness of existing controls and identifying areas for improvement. Organizations should engage cybersecurity experts to assist in this process, ensuring that their assessments are both comprehensive and informed by the latest industry standards.
- **Enhance Third-Party Due Diligence**: Organizations must update their due diligence processes for TPSPs, requiring compliance with rigorous cybersecurity standards. This includes not only assessing the cybersecurity measures in place but also ensuring TPSPs maintain those standards over time.
- **Develop a Culture of Cybersecurity Awareness**: Organizations should invest in comprehensive training programs that include practical scenarios related to AI threats. Employees at all levels should be able to recognize and respond to potential risks, fostering a culture of vigilance and accountability.
- **Implement Robust Monitoring Solutions**: Organizations should establish effective monitoring processes that can identify security vulnerabilities and unusual behaviors promptly. Companies should consider leveraging AI-driven monitoring solutions to enhance their capabilities in detecting and responding to threats in real time.
- **Adopt Data Minimization Practices**: Organizations should prioritize data minimization as a key component of their data governance frameworks. This includes implementing policies for the responsible and timely disposal of NPI while remaining compliant with data retention requirements.
- **Stay Informed and Adapt**: The regulatory landscape is evolving rapidly. Organizations must stay informed about changes in regulations and emerging threats, adapting their compliance programs accordingly. The best way to stay connected is by engaging with industry groups, keeping up with relevant publications, and attending conferences such as Winston & Strawn's upcoming Compliance Symposium on December 10 in New York.

CONCLUSION

DFS's latest guidance letter marks a key shift for compliance professionals in the financial services sector and beyond. It provides a comprehensive roadmap for navigating the challenges posed by AI technologies, enabling organizations to strengthen their cybersecurity posture and better protect sensitive information. As organizations look to implement these strategies, consulting cybersecurity experts and compliance professionals will be crucial. Effectively adapting to these new standards not only enhances an organization's defenses but also fosters trust among regulators, clients, and stakeholders. By proactively addressing these issues, organizations can demonstrate their commitment to maintaining robust cybersecurity practices and safeguarding the interests of all involved.

Please contact the authors or your Winston & Strawn relationship attorney if you have any questions or need further information.

---

[1] N.Y. Dep't Fin. Servs., *Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks* (Oct. 16, 2024), https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks ("DFS Industry Letter").

[2] *See* N.Y. C.R.R. § 500.1(e) (stating that DFS regulations apply to "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies").

[3] *See* DFS Industry Letter n.5.

[4] *See* N.Y. C.C.R. § 500.1(p) (defining risk assessment).
7 Min Read

Authors

Richard Weber

David A. Kolansky

Josh Roth

Related Topics

Cyber Security

New York State Department of Financial Services (DFS)

Related Capabilities

Government Investigations, Enforcement & Compliance

Privacy & Data Security

Artificial Intelligence (AI)

Financial Crimes Compliance

Technology, Media & Telecommunications

Related Professionals

Richard Weber

David A. Kolansky

Josh Roth

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.