Insights

U.S. Treasury Issues Report on Artificial Intelligence on Specific Cybersecurity Risks in the Financial Services Sector

April 4, 2024

By: Michael J. Messaglia

The U.S. Department of the Treasury recently released a comprehensive report on managing artificial intelligence (AI) specific cybersecurity risks within the financial services sector. The Report was issued as just one of the steps mandated by Executive Order 14110 on *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. The Report not only highlights the current state of AI implementation within financial institutions but also underscores the evolving landscape of AI technologies and their implications for risk management and regulatory compliance.

The Report reveals disparities in AI adoption based on institutional size, with many institutions, regardless of size, engaging third-party providers. Notably, smaller institutions often lack the resources and expertise to develop AI models in-house, relying solely on third-party solutions. Moreover, the rapid pace of AI development has led to a talent gap in the workforce, making it challenging for institutions to build and sustain an AI workforce.

Treasury noted that the adoption of AI, including Generative AI, holds promise for improving cybersecurity and anti-fraud management functions, but challenges persist, including the high cost and difficulty of validating Generative AI models. Furthermore, the lack of data sharing among financial institutions hampers the effectiveness of AI in fraud detection. Collaboration is essential to aggregate fraud data and develop sophisticated fraud detection tools, especially as fraudsters leverage AI and machine learning technologies.

Regulatory agencies emphasize the importance of effective risk management and governance in AI implementation, urging financial institutions to manage AI-related risks in line with existing laws and regulations.

The Report highlights best practices for managing AI-specific cybersecurity risks, including:

- Embedding AI-specific risk management within enterprise risk management programs with a focus on identifying, measuring, monitoring, and managing AI-related risks.
- Integrate AI into risk management functions which may include identifying lead or responsible officer.
- Expand due diligence processes when evaluating AI vendors, including inquiries about AI technology integration, data privacy, model validation, and maintenance practices.
- Implement and extend multifactor authentication as AI may thwart existing authentication practices.

Although not a focus of the Report, Treasury highlighted additional risks such as biased decision-making, unethical applications, and erroneous outputs. To mitigate these risks, the Report emphasized the importance of implementing Model Risk Management (MRM) practices. Furthermore, Treasury cautioned that AI systems may not be appropriate for high-assurance applications that necessitate consistent and impartial decision-making.

In conclusion, the U.S. Treasury's Report serves as a critical resource for financial institutions as they navigate the complexities of AI-related risks.

Disclaimer. The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.

*** The author used artificial intelligence to assist in the preparation of this Alert.*