

Adversarial AI: Meeting Emerging Risks and Threats in Financial Institutions

BLOG POST

Adversarial AI: Meeting Emerging Risks and Threats in Financial Institutions

October 15, 2026

| [Download PDF](#)

Share:

By Brad Robinson, CSBS Senior Director, Cybersecurity Policy and Supervision

Recent developments in the field of artificial intelligence (AI) are generating a considerable amount of excitement. In a time where news of exciting advances in AI is a near-daily occurrence, there is reason for optimism when thinking of how AI might improve internal administrative and operations processes, drive meaningful change in how customers interact with our financial institutions, and make our organizations more secure.

However, there is also reason for concern. The power and capabilities that could benefit the financial sector also introduce significant risks and threats. There is a sense of urgency in the frequency and tone of bulletins and alerts coming from government cybersecurity agencies and industry organizations, and financial institutions are, in many ways, now entering a time when they must enhance their focus on cybersecurity to address the growing threat of adversarial AI use.

CSBS has identified three primary areas of concern for financial institutions.

First, ***AI is enabling increased vulnerability discovery capabilities, which will change the volume and nature of patching.*** Powerful frontier AI models can identify large volumes of vulnerabilities, including zero-days, and are reportedly capable of generating proof-of-concept exploits and even vulnerability chaining for identified vulnerabilities. While these capabilities will greatly benefit security teams, they will also drive a necessary change in how institutions approach patching and vulnerability management. There are concerns over increasing patch volume, vulnerability severity and prioritization, and the capabilities of smaller institutions and the service providers that often support their efforts.

To respond to increasing vulnerability volume, institutions should reexamine existing patch and vulnerability management processes, as well as strengthen fundamental supporting cybersecurity controls. Faster patching alone will ***not*** be sufficient to address risks from the vulnerability discovery capabilities of AI.

The use of AI to create sophisticated social engineering, phishing, vishing, and deepfakes is yet another concern for financial institutions. Quite simply, AI makes social engineering more efficient and effective. Today's AI is powering the automation of victim reconnaissance by parsing social media and open-source information to profile and target victims - all at a speed and scale that no human can match.

Phishing emails, vishing, and deepfakes are becoming increasingly effective, all due to the injection of AI into the development and execution of campaigns. Today's attempts are dangerous, sophisticated, and targeted, and the wide availability and growing utilization of AI by threat actors will only serve to make these attack vectors more exploitable at scale in the future.

Finally, ***AI is automating the design, development, and deployment of malware***. There is evidence that AI is being utilized in all phases of the attack lifecycle. Threat actors use AI to streamline reconnaissance and victim targeting. There is also growing concern over the emergence of new malware families that leverage AI to more dynamically adapt to individual environments in which they are introduced. Threat actor groups are developing AI-generated or AI-assisted malware, and there is reason to believe that by many Ransomware-as-a-Service platforms are using AI, making these services an even more attractive option for less sophisticated actors. A key point of risk for financial institutions is the prospect of AI-driven or AI-enhanced malware creating new, significant challenges for existing cyber defense mechanisms, increasing the overall volume and complexity of attacks and opening doors further for new threat actors.

Currently, there are a number of recommendations from government cybersecurity agencies and industry groups to address these emerging threats. CSBS has outlined nine fundamental recommendations for financial institutions that closely mirror many of these recommendations. These actions, which are an amalgamation of recommendations from [FS-ISAC](#), the [European Central Bank](#), and other sources, address:

- Strengthening the institution's security perimeter
- Reevaluating vulnerability prioritization and shortening patching timelines
- Validating and updating critical asset inventories
- Replacing end-of-life (EOL) technology and strengthening EOL management processes
- Enforcing strong user access controls and privilege management
- Governing the use of open-source software
- Using available AI models for defense
- Verifying that third-party risk management practices are fit for purpose
- Building and testing robust incident response and resilience capabilities

In December 2025, CSBS released [Cyber Hygiene Fundamentals for Financial Institutions](#), which provides additional foundational detail on many of the concepts contained in the recommended actions noted above. In addition, the [CSBS Ransomware Self-Assessment Tool](#) is an excellent resource for bank and nonbank institutions of all sizes to use to identify areas requiring attention to address readiness for confronting ransomware and other cyber threats.

We recommend that all institutions review these documents now to support preparations for addressing today's rapidly evolving threat environment.

Related Topics
[Cybersecurity](#)

Related Posts