

The Growing Faultline in Cyber Defenses: Third-Party Service Providers in the Era of Frontier AI

Kristin Royster | Sept. 1, 2026

Banks have invested billions in cybersecurity over the past several decades, making the financial sector more secure and resilient. But the threat of systemic cyber risk is increasingly concentrated outside bank walls – in the third-party service providers supporting core financial operations.

That challenge is more urgent as frontier AI models accelerate vulnerability discovery and compress the time available to identify, prioritize and remediate weaknesses. Banks can strengthen their own systems, but they are dependent on third parties to fix vulnerabilities in software and platforms they do not control. The speed with which third parties fix their systems is critical as attackers increasingly use AI tools to exploit vulnerabilities more quickly. Over the past several years, the average timeframe from when a vulnerability is publicly disclosed to active exploitation has decreased from 53 **days** in 2024 to 22 **hours** in 2026.[1] This makes strong, multi-layered defenses paramount, and third parties need to double down on foundational security and resilience practices.

Financial regulators acknowledge these risks. A recent Federal Reserve Board staff report describes third-party service providers as "a hidden cyber fault line within the financial system."[2] The report notes that these providers "often have greater cyber vulnerabilities than the financial institutions they serve."[3] Concentration risk makes the problem more acute. A relatively small number of technology firms, including major cloud service providers, support a large share of the financial sector. Because that is the case, the potential effect of an outage or cyber incident at any one of those providers increases substantially and could have ripple effects across the industry.

[1] Zero Day Clock
[2] Chang, Jin-Wook et al., Cyber Vulnerabilities at Large US Financial Institutions and Their Third-Party Service Providers, November 2025, Finance and Economic Discussion Series (FEDS), Federal Reserve Board.
[3] Cyber Vulnerabilities at Large US Financial Institutions and Their Third-Party Service Providers

These risks are not hypothetical. In October 2025, a 15-hour Amazon Web Services outage caused cascading failures for thousands of its customers across multiple industries.[4] Through no fault of their own, these customers, including banks that had developed backup plans with AWS, experienced business disruptions, lost revenue and had to divert technology teams to execute new emergency backup plans. Despite incidents like this, third parties still operate without meaningful direct regulatory oversight to ensure they implement appropriate resilience measures and do not create additional risk. The 2025 Annual FSOC report noted this concern, saying: "as service providers play a larger role in supporting important functions of financial institutions, supervisory agencies should have the necessary tools to oversee the related safety and soundness risks."[5]

Federal banking regulators already have the authority to examine these companies under the Bank Service Company Act. Nevertheless, that supervisory framework has historically been lighter and less transparent than the one applied to banks, and it has not kept pace with the sector's growing reliance on technologies like cloud computing. Federal Reserve Vice Chair for Supervision Michelle Bowman recently stated that third-party risk management guidance should be updated and simplified. She also said the guidance should "reflect actual and future risk."[6] We agree.

To this end, now is the time for regulators to modernize their approach by focusing on core risks, reducing unnecessary regulatory burdens and sharpening exam focus on security and resilience at third parties critical to the financial system.

Several practical steps would help close this gap:

- Increase direct supervision of third-party providers that service large numbers of financial institutions and have a role in critical service delivery;
- Engage with banks to ensure that exams of service providers address timely security and resilience concerns; and
- Develop a streamlined and timely process to share service provider exam findings with banks so that resources can be used effectively.

Over time, frontier AI models will strengthen defenses by helping organizations identify and remediate weaknesses more quickly. In the near term, however, these capabilities expose institutions to greater risks. If key third-party providers are not prioritizing and providing transparency into their security program improvements and technology modernization plans with their bank customers – and if regulators lack sufficient visibility to confirm that this sharing is taking place – the financial sector's systemic exposure will continue to grow.

_____

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.

[4] What caused the AWS outage - and why did it make the internet fall apart?
[5] Financial Stability Oversight Council 2025 Annual Report, p.17
[6] Speech by Vice Chair for Supervision Bowman on artificial intelligence in the financial system - Federal Reserve Board