PUBLICATION

When it Rains it Pours: Lessons for Businesses Following the AWS Service Disruption

Authors: Matthew George White, Alexander Frank Koskey, III
October 24, 2025

On October 21, 2025, much of the internet stopped behaving as expected. The largest cloud provider in the world, Amazon Web Services (AWS), suffered a significant service disruption that rippled through countless businesses, including banks, insurers, and technology companies. It served as a stark reminder that even the most sophisticated vendors can experience disruptions, and when they do, the disruption lands squarely on the shoulders of the organizations that depend on them.

The AWS event came within hours of a new Industry Letter from the New York Department of Financial Services (NYDFS) reminding covered entities that third-party risk management isn't optional and that responsibility for cybersecurity and operational resilience cannot be outsourced. In addition to background information on and key takeaways from this week's AWS event, this alert provides regulated organizations that depend on cloud and technology vendors with practical guidance for managing third-party risk.

A Perfectly Timed Wake-Up Call

NYDFS's new Industry Letter, "Guidance on Managing Risks of Third-Party Service Providers," doesn't impose any new rules – it simply highlights a common message: you can delegate a function, but not accountability for that function. As they say, "Hiring a babysitter doesn't make you any less of a parent." Here, NYDFS emphasized that covered entities remain fully responsible for cybersecurity compliance, operational resilience, and consumer protection, including, without limitation, the following reminders.

- **Identification, Due Diligence, and Selection**: Covered entities must assess the cybersecurity risks a third-party service provider poses to the covered entity's information systems and National Provider Identifier (NPI). This should include policies and procedures outlining how such risks are evaluated and minimum cybersecurity standards required for engagement. Third-party service providers should be classified based on their risk profile, considering things such as system access, data sensitivity, and how critical the service is to the covered entity.

- **Tailored Risk Plan**: NYDFS reminds covered entities that they should develop a tailored plan to mitigate the risks posed by each third-party service provider. This includes considerations such as the third-party service provider's reputation in the industry, the access controls implemented for its own systems and data, whether the service provider maintains and regularly tests its incident response and business continuity plans, and the provider's practices for selecting, monitoring, and contracting with downstream service providers.

- **Contracting**: The Industry Letter also reminds covered entities of considering certain baseline contract provisions in their third-party service provider agreements, including obligations to encrypt data in transit and at rest, timely notice to the covered entity upon the occurrence of a cybersecurity event, data location and transfer restrictions, use of subcontractors, and restrictions on the use and sharing of data.

The letter encourages covered entities to think of third-party risk not as a box-checking exercise, but as an ongoing governance obligation that stretches across the vendor lifecycle. The message is clear: oversight doesn't end once the ink on the contract dries.

The guidance also broadens the conversation beyond cybersecurity incidents to include operational outages, cascading failures, and so-called "fourth-party" risk, or the risks related to the vendors your vendors rely on (or nth party risk – going on and on down the line). AWS's event provided a real-time example of why that distinction matters. A single service disruption in one region can reverberate across industries, leaving even well-prepared institutions scrambling for contingencies.

Why This Matters – and Not Just in New York

For financial institutions, insurers, and fintech companies subject to NYDFS oversight, the message is simple: covered entities have become more reliant on third-party vendors, and vendor management should be as rigorous as internal risk management. For everyone else, this guidance signals a growing regulatory expectation across industries – from the Securities and Exchange Commission's cyber disclosure rules to the Consumer Financial Protection Bureau's emphasis on third-party supervision. The concept is spreading: regulators no longer see third-party risk as a separate issue from cybersecurity or operational resilience. They see it as one and the same.

This matters because modern enterprises run on an invisible lattice of third-party providers, including cloud providers, Software as a Service (SaaS) platforms, payment processors, and IT vendors. Outages that once seemed rare are now recurring reminders that dependency is a double-edged sword. The AWS incident may have lasted only hours, but the reputational and operational impacts for some companies were immediate, and regulators were watching to see how those companies responded.

What You Should Be Doing Now

For organizations that depend on cloud and technology vendors, this is a moment to pause and re-evaluate. Ask yourself: if one of your key vendors went offline for 12 hours, how quickly could you pivot? Do you know which services would be affected? Have you tested your continuity plan – or would you be testing it for the first time mid-crisis? Have you simulated such an incident during a tabletop exercise?

NYDFS expects covered entities to map their vendor ecosystem, understand dependencies, and document how they monitor and manage those relationships. Contracts should clearly define uptime expectations, incident-notification obligations, and exit rights if resilience failures persist (along with expectations for remediation assistance and who will pay for it). But paper alone isn't protection; regulators want to see a living oversight program, one that boards and executives actively review and test.

In practical terms, that means integrating third-party oversight into your regular cybersecurity governance, including tracking vendor performance metrics, requiring resilience attestations, and incorporating vendor-failure scenarios into tabletop exercises. The goal is not just to meet compliance expectations but to build confidence that your business can stay operational when (*not if*) a major provider experiences disruption.

The Takeaway – You Can't Outsource a Storm

The AWS service disruption didn't expose a new risk; it simply made an existing, abstract risk tangible. For years, regulators and risk professionals have warned that "the cloud" doesn't make risk disappear, it just moves it off-premises. NYDFS's guidance reaffirms that your compliance obligations follow you wherever your data and systems reside.

At the end of the day, even when your data lives in the cloud, your accountability sits firmly at your doorstep. If your organization hasn't revisited its third-party risk management program, cloud contracts, or resilience testing

lately, now is the time. The authors, Matt White and Alex Koskey, routinely help clients evaluate vendor relationships, strengthen operational resilience, and prepare for regulatory scrutiny before the disruptions occur (and also assist clients in responding when they do). If a third-party failure or outage does happen, our team can help you respond quickly, mitigate downstream risks, and engage regulators from a position of strength.

For more information or to discuss updating your vendor governance and resilience strategy please contact Matt White, Alex Koskey, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.