

Black October

What Insurance Leaders Need to Know

What happened, why it matters, and what insurers should do now.

Current as of October 25, 2026

What Black October revealed

October 2026 brought a wave of major cybersecurity vulnerability disclosures, highlighting how quickly the threat landscape is evolving. While many of the underlying incidents began months earlier, the **speed** at which newly disclosed vulnerabilities can be exploited is accelerating. According to Rapid7, attackers exploited severe vulnerabilities an average of just three days after disclosure in Q3 2026.

For insurers, the implications extend beyond their internal systems. Third-party administrators, MGAs, technology providers and other vendors may introduce vulnerabilities that put sensitive policyholder information and critical business operations at risk.

The challenge isn't just identifying vulnerabilities. It's having the visibility, governance and processes to respond before attackers do.

3

DAYS

Average time from disclosure to exploitation of severe vulnerabilities, Q3 2026

Source: Rapid7

Is your organization prepared to respond that quickly?

The week in one table

EVENT	WHAT HAPPENED	INSURER EXPOSURE	DAY
PHP2Shell	Two critical PHP flaws, found with AI, allowed server takeover without a login. Exploited within hours of disclosure.	Portals and websites run by you or your vendors	1
AI agent intrusions	One attacker's AI agents breached 100+ companies for about \$50 each. Banks found AI agents using customer logins.	Policyholder and agent portals, account takeover	2
Railway, LiteLLM and others	Cloud and AI platforms leaked or stole API keys and credentials.	AI pilots, developers and insurtech vendors	3
PwC learning vendor	A vendor hosting employee learning records was breached, with an extortion group claiming 590 GB.	"Low-risk" vendors with SSO access and employee data	4

Other notable disclosures the same week included critical GitLab flaws, Node.js security releases, compromised certificate keys at eMudhra, a joint FBI and CISA warning on the SafePay ransomware group, and tampering with AOMEI Backupper's update servers that dated back to May. Each calls for the same discipline. **Know what you run, patch fast and ask your vendors.**

Four lessons that will outlast the headlines

01

The window between disclosure and attack is gone.

AI tools now find flaws and build attacks in hours. Insurers that patch on a monthly cycle, or wait for a portal, claims or policy administration vendor to tell them, leave policyholder-facing systems exposed for too long.

02

Your exposure is mostly someone else's system.

Nearly every event reached organizations through a platform they didn't run. For insurers, that means TPAs, MGAs and insurance technology providers. Third-party risk management has to be an ongoing operation, not an annual questionnaire.

03

Credentials are the prize.

Agent and policyholder portal logins, API keys linking rating and claims systems, and integration tokens held by vendors all lead to sensitive policyholder data. Every credential needs an owner, a purpose and a way to rotate it quickly.

04

Regulators will ask what you already had in place.

Unrotated tokens, compromised logins and unpatched VPNs did much of the damage, and these are the controls NYDFS Part 500 and state insurance data security laws already expect. Insurers whose basics were in place, and documented, came through best.

Four actions insurance leaders should prioritize now

These four areas drove most of Black October’s exposure for insurers, and they’re where boards and examiners are most likely to focus.

PRIORITY	WHAT TO DO NOW	WHAT TO ASK YOUR TEAM FOR
Vulnerability management	Set a patch target measured in days, not weeks, for internet-facing systems, including portals and websites your vendors run for you	Time to patch critical flaws, and vendor confirmation after each major disclosure
Third-party risk	Map which TPAs, MGAs and technology providers can reach your systems or policyholder data, and tier oversight by access rather than contract size	A current vendor access inventory and dated follow-ups after each vendor incident
Credential security	Require phishing-resistant MFA on remote, admin and vendor logins, and keep API keys in a vault with an owner and a rotation plan	A credential inventory with owners, and a list of documented MFA exceptions
AI governance	Set written rules for the AI tools and AI agents used by employees, vendors and policyholders, including how agents may access accounts	An approved-use policy and a list of AI tools that touch insurance data

Five questions leadership should ask this quarter

- 1 How quickly can we patch an internet-facing system once a critical flaw is announced, and how do we know our vendors can match it?
- 2 Which vendors can reach our systems through SSO, APIs or stored keys, and when did we last review them?
- 3 Is MFA on for every remote, administrative and vendor login, with no exceptions we haven't documented?
- 4 Do we have written rules for AI tools and AI agents, and do employees and policyholders know them?
- 5 If a vendor told us tomorrow that our data was stolen, could we meet a 72-hour regulatory notice?

FOR DFS-REGULATED ENTITIES

DFS’s May 2026 guidance named AI-driven change as a trigger for a heightened threat environment, and Black October fits that description. Two actions will matter most at your next exam. **Update your Part 500 risk assessment** to reflect what this month changed, and **keep a dated record** of how you responded to each event, including vendor follow-ups. That record also supports your April 15 certification.

How FiveM can help

FiveM’s view is simple. There will be another Black October, and the organizations that handle it best won’t be the ones reading the most headlines. They’ll be the ones that already know what they run, who runs it for them, and which credentials open which doors. That’s the work FiveM does with insurers and financial services firms, from vendor due diligence and external exposure reviews to AI governance and documentation that stands up to DFS and NAIC examiners.

The October Cyber Brief is coming soon. It will go deeper on Black October and what’s likely to follow.

Do you know where your organization’s biggest cybersecurity exposures are?

FiveM’s Security & Regulatory Assurance team can help you find them. Book a 30-minute call, and we’ll help you decide where to start.

SOURCES

- SecurityToday: Black October, many attacks had been running for months (October 22, 2026)
 - CNBC: AI’s Black October, critical PHP flaws set off global security scramble (October 23, 2026)
 - 404 Media: AI is changing everything about hacking (October 22, 2026)
- UK NCSC: Preparing for a vulnerability patch wave (May 2026)
 - Rapid7: Q3 2026 threat update, attackers exploiting vulnerabilities within 3 days
 - NYDFS: Heightened Cybersecurity Threat Environment Guidance (May 21, 2026)