NEWS RELEASE

Rapid7 2026 Cybersecurity Trends Outlook: Geopolitical Tensions and Insider Threats Among Top Risks

2025-12-11

BOSTON, Dec. 11, 2025 (GLOBE NEWSWIRE) -- **Rapid7, Inc.** (NASDAQ: RPD), a leader in threat detection and exposure management, today released its top cybersecurity predictions for 2026 from executives **Raj Samani**, **Sabeen Malik**, and **Rob Dooley** during its **Top Cybersecurity Predictions for 2026 webinar**. Rapid7's insights reveal the myriad impacts of geopolitical conflicts, highlight insiders as an increasing cybersecurity threat, and emphasize that contextual awareness will be vital for effective cyber defense in the year ahead.

"Cybersecurity is intelligence. It's the ability to gather signals from the noise and respond appropriately," said Samani, Rapid7's chief scientist. "It begins with leveraging and utilizing actionable, unified cyber intelligence; looking for solutions that give you that unified approach and actionable outcomes that you can implement within your own environment."

Rapid7's 2026 security predictions

1. Geopolitical fault lines will redraw the cyber battlefield, as tensions between nation-states spill over into the private sector. The geopolitical landscape in 2026 will bring with it an expanding use of digital attacks beyond national borders, making private organizations in critical supply chains even more prone to becoming proxy targets for state-aligned groups. These attacks will blend third parties and nation-state actors while they are engaging in espionage and economic sabotage, allowing governments plausible deniability for real-world disruption. Organizations can use curated threat intelligence to track geopolitical flashpoints, emerging APT tools, and evolving attacker infrastructures to stay ahead of the threats to their critical infrastructure.
2. Insider threats will dominate breach root causes, from simple negligence to monetized access selling. By 2026,

threat actors won't always break in; they'll be invited. Disgruntled insiders and careless employees will become key vectors for compromise, especially as economic and cultural pressures continue to intensify. It will be critical that organizations establish behavior baselines across users and roles to flag anomalous access, downloads, and logins, as well as regularly review privilege models to limit unnecessary access and reduce potential blast radius.

3. Context will become the new currency of cyber performance. You can't successfully protect what you don't fully understand. As AI scales attacks, defenders need context, not just alerts. Integrating exposure management and detection capabilities is crucial for faster triage, smarter response, and measurable impact. Demonstrating the value of the security stack will come down to the metrics that really matter: time saved, dwell time reduced, risks remediated, and workflows accelerated.

"We have some really aggressive actors that are trying to exploit whatever it is they can. Still, humans at the end of the day are going to see more sophisticated attacks using things like AI," said Malik, Rapid7's vice president of Global Government Affairs and Public Policy. "Organizations must build their security technologies on a foundation of understanding the separation between the human elements and computing elements across their attack surface."

"In 2025, one of the predictions we didn't make was the speed of consolidation," said Dooley, general manager for Rapid7's Asia-Pacific Japan region. "Consolidation doesn't mean that you have to pick everything from one vendor or one platform. True consolidation moving ahead is going to be having an open platform whereby you can ingest telemetry from the tools that you've invested in, but you can consolidate [the data] and provide that context [for decision-making]."

Reflecting on a year of innovation

This outlook caps a year of accelerated innovation for Rapid7. The company introduced new research insights on **access brokers** and the **global threat landscape**, delivered key launches including **Incident Command** and **Vector Command**, and expanded **Managed Detection and Response** (MDR) coverage for Microsoft environments, advancing its mission to help organizations manage risk and detect threats across increasingly complex environments.

About the Top Cybersecurity Predictions webinar

The Rapid7 Top Cybersecurity Predictions webinar is held annually in December to provide Rapid7 customers and the greater community with the expert insights and recommendations needed for proactively addressing the latest trends and threats in cybersecurity. During each year's webinar, a team of Rapid7 executives from various global locations are joined by an expert moderator. This year's webinar was moderated by British journalist and consultant **Philip Ingram**, who has built on a long and senior military career in intelligence, counterintelligence and

security, and as an operational planner.

A replay of Rapid7's Top Cybersecurity Predictions for 2026 webinar can be viewed **here**.

About Rapid7
Rapid7, Inc. (NASDAQ: RPD) is on a mission to create a safer digital world by making cybersecurity simpler and more accessible. We empower security professionals to manage a modern attack surface through our best-in-class technology, leading-edge research, and broad, strategic expertise. Rapid7's comprehensive security solutions help more than 11,000 global customers unite cloud risk management with threat detection and response to reduce attack surfaces and eliminate threats with speed and precision. For more information, visit our **website**, check out our **blog**, or follow us on **LinkedIn** or **X**.

Rapid7 Media Relations
Alice Randall
Director, Global Communications
press@rapid7.com
(857) 216-7804

Rapid7 Investor Contact
Matt Wells
Vice President, Investor Relations
investors@rapid7.com
(617) 865-4277

Source: Rapid7