NEWS RELEASE

Rubrik Reveals 90% of Global IT and Security Executives Report Cyberattacks in the Past Year

2025-04-22

Data sprawl drives spike in cyber incidents across AI, cloud, SaaS, and on-premise environments, according to Rubrik Zero Labs Report

PALO ALTO, Calif.--(BUSINESS WIRE)-- New research from Rubrik Zero Labs finds that organizations are facing a wave of cyberattacks, with 90% of IT and security leaders reporting cyberattacks in the past year. The report, "**The State of Data Security in 2025: A Distributed Crisis**," reveals the hazards that hybrid environments are creating, leading to a cloud security crisis that organizations are unprepared to address.

"Many organizations that move to the cloud assume their providers will handle security," said Joe Hladik, Head of Rubrik Zero Labs. "The persistence of ransomware attacks, coupled with the exploitation of hybrid cloud vulnerabilities, shows that threat actors are always one step ahead. Companies must take action and adopt an attacker's mindset by identifying – and protecting – the most valuable data before it's too late. The need for a data-centric security strategy that prioritizes visibility, control, and quick recovery has never been more urgent."

The Frequency and Impact of Cyberattacks Accelerate

Cyberattacks are a constant threat:

- Nearly one fifth of organizations globally experienced more than 25 cyberattacks in 2024 alone, according to IT and security leaders – an average of at least one breach every other week.
- The most common attack vectors cited were data breaches (30%), malware on devices (29%), cloud or SaaS

breaches (28%), phishing (28%), and insider threats (28%).

- Consequences of these attacks include:
  - 40% of respondents reported increased security costs.
  - 37% noted reputational damage and loss of customer confidence.
  - 33% experienced a forced leadership change following a cyber incident.

AI, Cloud Adoption and Greater Data Complexity Create New Challenges

Protecting sensitive data across multiple systems has become increasingly nuanced as the widespread adoption of AI has significantly exacerbated the challenge of data sprawl. An overwhelming 90% of IT and security leaders report managing hybrid cloud environments, and half of IT leaders say the majority of their workloads are now cloud-based.

As a result, "**The State of Data Security in 2025: A Distributed Crisis**" found:

- 35% of respondents cite securing data across these varied ecosystems as their top challenge, followed by a lack of centralized management (30%), and a lack of visibility and control over cloud-based data (29%).
- 36% of sensitive files in the cloud are classified as high risk and are largely composed of Personally Identifiable Information (PII), such as Social Security numbers and phone numbers; followed by digital data and business data, such as intellectual property and source code. (Rubrik telemetry data)

Ransomware and Identity Threats Evolve in Tandem

Ransomware remains a persistent and evolving threat:

- Of the organizations that experienced a successful ransomware attack last year, 86% admitted they paid a ransom to recover their data.
- Nearly three-quarters (74%) said threat actors were able to partially compromise backup and recovery systems, while 35% said their systems were completely compromised.

Identity threats are intensifying, fueled by the complexity of today's hybrid environments:

- With 92% of organizations using between two and five cloud and SaaS platforms, attackers are exploiting weak points in identity and access management to move laterally and escalate ransomware attacks.
- Insider threats – often driven by compromised credentials – were cited by 28% of IT leaders, underscoring the growing difficulty of maintaining strong access controls across distributed systems.
- Rubrik telemetry reveals that 27% of high-risk sensitive files contain digital data such as API keys, usernames, and account numbers – exactly the kind of information threat actors seek to hijack identities and infiltrate

critical systems.

To read the full report, visit **https://zerolabs.rubrik.com/**. For more information, register for the webinar, **Notions Behind the Numbers: Viewpoints on Rubrik Zero Labs Latest Report**, taking place May 14, 2025 at 9 a.m. PT.

Methodology

"The State of Data Security in 2025: A Distributed Crisis" is based on insights from over 1,600 IT and security leaders across 10 countries (half of whom were CIOs or CISOs), conducted in partnership with Wakefield. The findings are amplified by Rubrik telemetry data, including an analysis of 5.8 billion total files across cloud and SaaS environments, with over 175 million sensitive files classified across customer environments. Data covers the period from January 1, 2024, through December 31, 2024.

About Rubrik

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information, please visit **www.rubrik.com** and follow **@rubrikInc** on X (formerly Twitter) and **Rubrik** on LinkedIn.

Media Contact:

Meghan Fintland
Head of Global PR, Rubrik
925.785.9192
Meghan.Fintland@rubrik.com

Source: Rubrik