NEWS RELEASE

Healthcare Organizations Lose 20% of their Sensitive Data in Every Ransomware Attack, Reports Rubrik Zero Labs

4/30/2024

- Healthcare organizations experienced 50% more encryption events than the global average across 2023
- Cloud continues to drive inherent risk and security blind spots as 70% of all data is typically not machine readable by security appliances
- Leadership changes following cyberattacks are on the rise, with major personnel changes reported by 44% of organizations — up from 36% in 2022.

PALO ALTO, Calif.,--(BUSINESS WIRE)-- Recent cyber incidents demonstrate the healthcare industry continues to be a prime target for ransomware hackers. New research by Rubrik Zero Labs reveals that ransomware attacks produce larger impacts against these healthcare targets. In fact, the report estimates that one fifth of all sensitive data belonging to healthcare organizations is impacted in each ransomware attack.

Rubrik Zero Labs' new "**The State of Data Security: Measuring Your Data's Risk**" report offers insights on real-world risks against data as the pace and volume of cyber events continues to increase globally, aided by the explosion of data in the cloud and the realities of modern computing environments. Rubrik Zero Labs studies the challenges organizations' face to protect their crown jewels — their data — as well as how to reduce data risk and prepare for the evolving risk cycle before, during, and after a cyberattack.

"Despite the fallout of cyberattacks dominating headlines, data risk is an issue that continues to be murky — especially in terms of what security teams can actually change and what they cannot," said Steven Stone, Head of

Rubrik Zero Labs. “With this report, we aim to provide quantifiable insights that IT and security leaders can bring back to their organization to drive greater cyber resilience-in particular with their partners in the business and governance teams. The more we talk about cyber threats like ransomware, and its impact on industries like healthcare, the more we can collaborate to minimize the risk calculus and ultimately beat cyber attackers trying to impede our businesses.”

The Rubrik Zero Labs research unit pairs Rubrik telemetry across its customer base of more than 6,100 organizations with findings from a survey conducted by Wakefield Research of more than 1,600 IT and security leaders — half of which are CIOs and CISOs. Additionally, this study incorporated data from two Rubrik partner organizations and five other research organizations in an effort to provide the most objective findings. With core focuses including the cyber threat landscape in the healthcare industry, cloud data security blind spots, and ransomware, key findings include:

Healthcare Far Surpasses the Global Average in Sensitive Data

- Rubrik observed that healthcare organizations secure 22% more data than the global average.
- A typical healthcare organization saw their data estate grow by 27% last year.
- A typical healthcare organization has more than 42 million sensitive data records — 50% more sensitive data than the global average of 28 million.
- Sensitive data records in observed healthcare organizations grew by more than 63% in 2023 — far surpassing any other industry and more than five times the global average (13%).

Ransomware Produces Outsized Impacts Against Healthcare

- Ransomware attacks against observed healthcare organizations have an estimated impact of almost five times more sensitive data than the global average.
- This equates to an estimated 20% of a typical healthcare organization's total sensitive data holdings impacted every time there is a successful ransomware encryption event, compared to 6% for an average organization.
- Virtualization really matters for healthcare and ransomware: 97% of all encrypted data in Rubrik observed healthcare organizations last year occurred within virtualized architecture compared to 83% across all industries.

As Cloud Becomes More Widely Adopted, New Security Blind Spots Emerge

- Organizations are becoming more dependent on the cloud. In 2023, Rubrik observed that cloud architecture stored 13% of an organization’s data, compared to 9% in 2022. Comparatively, on-premises declined from 77% in 2022 to 70% in 2023.
- Of the external organizations victimized in a cyberattack in 2023, many were attacked across multiple aspects

of their hybrid environment with 67% of attacks impacting SaaS data, 66% for the cloud, and 51% for on-premises locations.

- The cloud comes with inherent risk based on security blind spots and vulnerable sensitive data, according to Rubrik Telemetry:
    - Blind spot #1: 70% of all data in a typical cloud instance is object storage, which typically has a far lower security coverage compared to other areas.
    - Blind spot #2: 88% of all data in object storage is not confirmed as machine readable or covered by prominent security technologies and services.
    - Blind spot #3: More than 25% of object storage data is subject to regulatory or legal requirements, such as protected health information (PHI) and personally identifiable information (PII).

Ransomware Continues to Wreak Havoc across Organizations — and IT and Security Teams

- 94% of IT and security leaders reported their organization experienced a significant cyberattack last year, and on average faced 30 attacks in that timeframe. One-third of these victims endured at least one ransomware attack.
- 93% of external organizations that endured a ransomware attack reported paying a ransom demand, with 58% of these payments motivated primarily by threats to leak stolen data.
- 96% of senior IT and security leaders reported changes to their emotional and/or psychological state as a direct result of a cyberattack, with 38% worrying over job security.
- Leadership changes increased following cyberattacks, reported by 44% of organizations — up from 36% in Rubrik Zero Labs' Fall 2022 report "**The State of Data Security: The Human Impact of Cybercrime**."

Rubrik Zero Labs, the company's data security research unit formed to analyze the global threat landscape, reports on emerging data security issues to give organizations research-backed insights and best practices to secure their data against increasing cyber events.

To read the full report, visit **https://rubrik.com/zero-labs**.

Report Methodology

"The State of Data Security: Measuring Your Data's Risk" report by Rubrik Zero Labs was commissioned by Rubrik and conducted by Wakefield Research among 1,625 IT and Security decision makers at companies of 500 or more employees. Respondents were made up of approximately half CIOs and CISOs and half VPs and Directors of IT and Security. The research was conducted in the US, UK, France, Germany, Italy, Netherlands, Japan, Australia, Singapore, and India between January 18 and January 30, 2024. None of these organizations are existing Rubrik clients.

The survey supplemented Rubrik telemetry, looking at more than 6,000 clients across 22 industries and 68 countries. The data includes over 42 exabytes of secured logical storage and more than 38 billion sensitive data records from January through December 2023.

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.

press@rubrik.com

Source: Rubrik