COHESITY

The State of Data Security and Management Report 2022

At a Glance

The first annual **State of Data Security and Management** report is based on a 2022 survey conducted by Censuswide of more than 2,000 IT and Security decision-makers (split nearly 50/50 between the two groups) from businesses in the United States, the United Kingdom, and Australia and New Zealand.

The survey found that ransomware attacks are on the rise globally, with nearly half of respondents indicating that their organization had been hit in the past six months. Two major factors surfaced as critical gaps in security strategies that put businesses at risk:

- A dependence on outdated, legacy backup and recovery infrastructure to manage and protect their data leaves organizations ill-prepared for the onslaught of sophisticated cyberattacks plaguing enterprises globally.
- A lack of collaboration between IT and Security Operations teams leaves organizations vulnerable to cyberattacks and risks compromising data security.

ADDITIONAL HIGHLIGHTS INCLUDE THESE FINDINGS:

Reliance on legacy technology is undermining how organizations respond to ransomware. Nearly half (46%) said their organization relies on primary backup and recovery infrastructure that was designed in, or before, 2010. When asked about the biggest barriers to getting back up and running after a successful ransomware attack, 34% said the lack of an automated disaster recovery system and 32% said antiquated backup and recovery systems.

Modernizing data management, protection, and recovery capabilities offers a path to strengthening security postures and multicloud operations. The top four "must have" measures that respondents would ask management for in 2022 are:

- Integration between modern data management and security platforms and AI-powered anomalous data and user alerts to provide early warning of attacks in progress (34%)
- Extensible platform for third-party applications for security operations and incident response (33%)
- Automated disaster recovery of systems and data (33%)
- Upgrading from legacy backup and recovery systems (32%)

Security should be a shared responsibility. More than four in five (81%) respondents overall somewhat or strongly agree that IT and Security teams should share responsibility for their organization's data security strategy. And although the threat of cyberattacks has increased, the level of collaboration has remained stagnant.

The ongoing tech talent shortage is making matters worse. When asked if the talent shortage is impacting the collaboration between IT and Security teams, 78% of respondents said it is having an impact.

For more detailed survey results and analysis, and to see what other organizations are doing to prevent and/or recover from ransomware attacks, read the full report:

Read the report