COHESITY

The State of Data Security and Management Report 2022

October 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 further validates 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A dependence on outdated, legacy backup and recovery infrastructure to manage and protect their data leaves organizations ill-prepared for the onslaught of sophisticated cyberattacks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. These outdated technologies were designed long before today's multicloud era.

A lack of collaboration between IT and Security teams leaves organizations vulnerable to cyberattacks and risks compromising data security.

Legacy infrastructure leaves companies vulnerable to ransomware attacks

In the world of data security and management, the early 2000s were simpler times. The good old days when backup and recovery solutions were just a box to be checked by IT teams in the event that disaster struck. And those disasters were usually the natural type — an earthquake shut down a data center, a hurricane damaged a facility — at that point, “ransomware” wasn’t even in our vocabulary and certainly didn’t dominate our news feeds.

Fast forward to 2022, and the world of cyberthreats looks very different. Today, ransomware is the fastest growing type of cybercrime. Analysts predict ransomware will attack a business every 2 seconds by the end of 2031[1]. And every time a cybercriminal succeeds, the organization attacked is damaged — financially and often reputationally. As data continues to grow at an unprecedented rate, how will legacy backup and data management solutions keep up?

Quite frankly, they won’t. You might be surprised that nearly half of survey respondents said their organization relies primarily on backup and recovery infrastructure designed in, or before, 2010. Another 5% revealed their organization relies on backup and recovery infrastructure built in the 1990s.

46%

said their organization relies primarily on backup and recovery infrastructure that was designed in, or before, 2010.

Although there’s been exponential growth in structured and unstructured data, and in the number of locations where data is stored, enterprises are still using this legacy technology even though managing and securing data environments has become much more complex. Forty-one percent of respondents stated they store data on-premises, 43% rely on public cloud, 53% use a private cloud, and 44% have adopted a hybrid model (some respondents are using more than one option).

“In 2022, the fact that any organization is using technology to manage their data that was designed in the 1990s is frightening given that data can be compromised, exfiltrated, held hostage, and it can create massive compliance issues for organizations,” said Spanswick. “In this survey, we found about 5% of respondents who said their organizations are relying on outdated data infrastructure, and this raises the question, how many other businesses are in the same situation around the world?”

[1,4] Cybersecurity Ventures. “Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031,” June 3, 2021.

> “IT and security teams should raise the alarm bell if their organization continues to use antiquated technology to manage and secure their most critical digital asset — their data. Cyber criminals are actively preying on this outdated infrastructure as they know it was not built for today’s dispersed, multicloud environments, nor was it built to help companies protect and rapidly recover from sophisticated cyberattacks.

BRIAN SPANSWICK, CHIEF INFORMATION SECURITY OFFICER, COHESITY

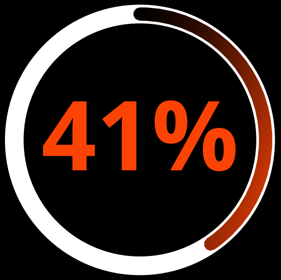
What keeps IT and Security teams up at night?

Cyber criminals are innovative, and they continue to create new malware. So despite concerted efforts to thwart ransomware attacks, these attacks are becoming both more sophisticated and more targeted. No matter what form they take, they always have the same goal: to disrupt business operations in the hopes victims will pay to restore order. No industry is immune. And because enterprises are even more attractive targets than consumers, your organization must proactively prepare for when, not if, cyber criminals come for your data.

Given that backdrop, respondents highlighted what they believe would be their biggest barriers to getting their organization back up and running after a successful ransomware attack. Respondents were asked to check all that apply and answered as follows:

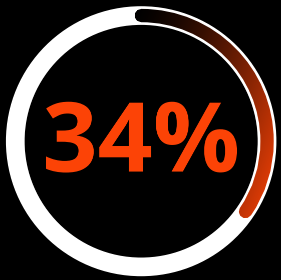
- Lack of integration between IT and security systems (41%)
- Lack of coordination between IT and Security teams (38%)
- Lack of an automated disaster recovery system (34%)
- Antiquated backup and recovery systems (32%)
- Lack of a recent, clean, immutable copy of data (32%)
- Lack of and timely detailed alerts (31%)

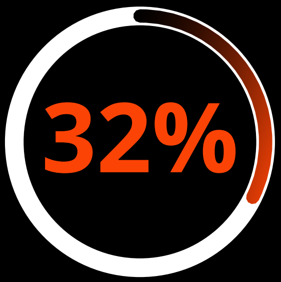
What's your biggest worry?



Lack of integration between IT and security systems

Lack of an automated disaster recovery system





Antiquated backup and recovery systems

What should management prioritize?

Respondents revealed that modernizing data management, protection, and recovery capabilities, in addition to increasing collaboration between IT and Security teams, offers a path to strengthening their organizations' security postures and multicloud operations. The top five "must have" measures respondents would ask management for are:

- Integration between modern data management and security platforms and AI-powered anomalous data access 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%)
- Rapid, organization-wide backup with in-transit data encryption (30%)

Integration between modern data management and security platforms and AI-powered anomalous data access alerts to provide early warning of attacks in progress

Security should be a shared responsibility

More than four in five (81%) respondents overall (86% of IT decision-makers and 76% of Security decision-makers) 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.

A lack of collaboration between IT and Security teams leaves organizations vulnerable to cyberattacks and risks compromising data security. Here's a breakdown of their responses:

- **When it comes to data security strategy, 86% of IT decision-makers and 76% of Security decision-makers somewhat or strongly agreed that responsibility should be shared.**
- **But effective collaboration isn't the norm. In fact, 1/3 of Security respondents characterized their collaboration with IT as "not strong."**
- **Even as the rate of cyberattacks has increased, 52% of respondents report that collaboration levels have either stagnated or dipped.**
- **This disconnect raises alarms, with 42% saying their organization is more exposed or much more exposed to cyberthreats.**
- **Consequences of this exposure could be swift and severe. When asked about their biggest fear if an attack took place, 42% were concerned about data loss, 42% about business disruption, 40% about losing customers, 32% about paying the ransom, and 30% about firings on both IT and Security teams.**

81%
AGREE

IT and SecOps should share responsibility for their organization's data security strategy.

> “Both IT decision-makers and SecOps should co-own the cyber resilience outcomes, and this includes an evaluation of all infrastructure used in accordance with the NIST framework for data identification, protection, detection, response, and recovery. Also, both teams need to have a comprehensive understanding of the potential attack surface. Modern data management platforms can close the technology gap, improve data visibility, help IT and SecOps teams sleep better at night, and stay one step ahead of bad actors who take great delight in exfiltrating data from legacy systems that can’t be recovered.”

BRIAN SPANSWICK, CHIEF INFORMATION SECURITY OFFICER, COHESITY

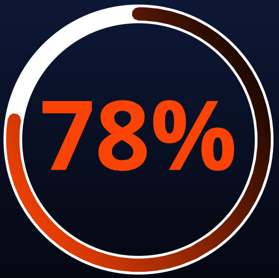
The good news

83% of respondents somewhat or strongly agree that if IT and Security collaborated more closely, their organization would be better prepared to recover from cyberthreats including ransomware attacks.

Talent shortage poses added challenges

It’s no secret the talent shortage is widespread, affecting all roles across all industries. In the technology sphere, its effect on data security may be less apparent than its effect on more visible parts of the organization. But its impact may be even more destructive.

- Nearly 60% of respondents expressed some level of concern about whether their IT and security teams would be able to mobilize efficiently to respond to an attack. Given that many teams are thinned out and requisitions remain unfilled, fewer qualified team members would be available to support a mobilization effort if one occurred.
- 47% respondents said their organization was the victim of a ransomware attack in the last 6 months. If the talent shortage persists, and the rate of ransomware attacks remains flat or increases, organizations will face mounting pressure.
- In a robust economic environment, opportunities for collaboration are more plentiful. But when IT and Security professionals are doing the jobs of multiple people, they may not prioritize collaboration — unless its benefits are made explicit.



The tech talent shortage is impacting collaboration between IT and Security teams.

The good news

Most IT and Security decision-makers do believe they should jointly share responsibility for their organization’s data security strategy. With this awareness comes a powerful opportunity — even if (or perhaps especially if) the talent shortage continues to cause strain.

It is also possible that as investments shift towards SaaS-based models, this will alleviate some of the talent shortage constraints. Combined with modern technologies that can automate security alerts and enable third-party extensibility with security leaders, the integration of IT and security systems could help IT and Security decision-makers share information and make dedicated decisions by looking at all the relevant operational data.

Conclusion

Data is a differentiator in the digital economy. That's why data has simultaneously become the most valuable and the most targeted business asset. Even as awareness of ransomware attacks is rising, more sophisticated and focused attacks increasingly target backup data and infrastructure, which continues to threaten enterprises worldwide. For businesses that do become compromised, steep financial loss is often compounded by customer distrust, and in the case of healthcare, risk to human life.

Given that half of respondents in our global survey indicated that their organization had been targeted in the past six months, it is critical that organizations close the gaps that put their security posture — and their business — at risk. Based on the survey results, companies must:

- **Invest in updating their backup and recovery infrastructure to manage and protect their data.**
- **Make collaboration between IT and Security teams a strategic imperative so that IT and Security systems integrate.**
- **Adopt modern technologies that can automate security alerts and enable third party extensibility with security systems.**

COHESITY