Cyber insurance for the enterprise

What to know about cost, coverage, and eligibility (and how Cohesity can help).

**COHESITY**

Introduction

The growing threat of ransomware and other cyberattacks is top of mind for IT and Security leaders.

In a 2023 global survey of over 3,400 IT and SecOps decision-makers[1], 93% said the threat of ransomware attacks to their industry had increased this year. Even more alarming, 45% said their organization had been the victim of a ransomware attack in the prior six months.

In a separate report by ESG[2], more than half of organizations said they paid a ransom to regain access to data, applications, or systems. Plus, the average ransom payment in 2023 is $1.54 million, nearly double the 2022 figure.

Yet even organizations that pay a ransom discover that doing so doesn't guarantee data recovery.
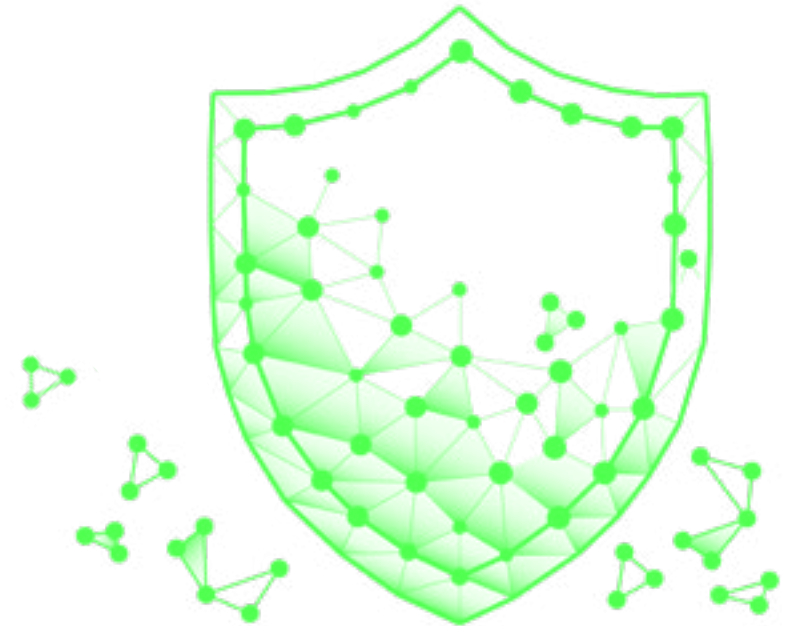
Only
16%
of organizations surveyed for the ESG report indicated they got all their data back after an attack.

Equally troubling, attackers have also been known to wipe—or delete—data, so even if payment is made, data is still lost forever.

The ransom payment is just one cost among many. Lost productivity, downtime, and reputational damage following an attack may be far costlier.

So that's the bad news.

1. The State of Data Security and Management Report 2023

2. Enterprise Strategy Group, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation

Cyber insurance: a key part of a comprehensive data security strategy

The good news? Organizations are fighting back. They're turning to modern data security and management solutions that increase their data, cyber, and business resilience.

And they're getting cyber insurance.

According to insurer Munich Re. as cited in Moody's September 2023 Special Report[3], the cyber insurance market is **projected to grow to $33 billion** in premiums by 2027, up from roughly $12 billion today.

And while cyber insurance doesn't **solve** the ransomware crisis, it's showing up more as part of a multilayered resilience strategy—especially as attacks and other cyber threats remain alarmingly frequent and severe.

Cyber insurance is an insurance policy that provides financial protection against losses resulting from cyberattacks, data breaches, and other cyber-related incidents. It may cover lost income, legal fees, data recovery fees, and the cost of hiring a public relations firm to help control damage to your company's brand.

In this eBook, we'll showcase Cohesity customers who have:

More easily qualified for cyber insurance

Successfully lowered their cyber insurance premiums

Implemented strategies to help strengthen their resilience

3. Moody's, "Cyber budgets increase, executive overview improves, but challenges lurk under the surface," 9/28/23

Cyber insurance is harder to get

With the average total cost of recovery from a ransomware attack approximately $4 million, it's no wonder that organizations have trouble securing cyber insurance.

Recent survey results from **Delinea** reveal that the number of companies taking more than six months to qualify for cyber insurance increased 21x from 2022 to 2023[4]. (The top reason smaller organizations had their claims voided or denied? A lack of security protocols in place.)

Cohesity's 2023 State of Data Security and Management Report echoes these challenges.

46%
of respondents said it's more difficult to get a cyber insurance policy today than it was three years ago.

4. Delinea 2023 State of Cyber Insurance Report: Exclusions Increasing as Costs, Reasons for Denial of Coverage Going Up, cited in CPO Magazine, 9/5/23

"Cyber insurance can be quite difficult to obtain, as I experienced during my first year at Bardel. Our policy covers the monetary loss of our clients' production data if it is impacted by a failure or a breach. But anything beyond that customer data is not covered by our policy, which is a concern to our organization. This is why we rely so heavily on making sure we have frequent backups on Cohesity…"

Arash Roudafshan, VP of Technology, Bardel Entertainment Inc.

"When I first took out cybersecurity insurance several years ago, the process was really quite simple. We just signed up for the insurance and paid the premiums. Now we have to complete a very detailed questionnaire that asks what kind of password policies we have, what multi-factor authentication methods we use, what our backup solutions are, how often we back everything up, if we test our backups regularly, and more."

Richard Humphreys, IT manager, The Southport School

Cohesity makes it easier to qualify

Even though the qualification process for The Southport School was onerous, Humphreys credits Cohesity with helping him qualify for coverage.

"I'm not convinced we could meet the minimum requirements for cybersecurity insurance anymore if we didn't have Cohesity in place," he stated.

Buying cyber insurance isn't like buying auto insurance, or any other insurance type. Applicants must meet numerous requirements—around internal security, people training, email security, and data protection policies, among others. According to the **Delinea survey**, the top reason organizations need to secure cyber insurance is because their board of directors or executive management teams require it.

Organizations generally need robust internal security controls and a modern backup and recovery solution in place to meet today's more stringent requirements.

Would your current data backup and recovery solution meet the necessary criteria?

With Cohesity, you could check off all these boxes with confidence:

- ☐ Snapshots can be kept in a virtually air-gapped area separate and isolated from the production network.

- ☐ Snapshots can be kept in a dedicated cloud backup service.

- ☐ Snapshots are encrypted.

- ☐ Snapshots are immutable.

- ☐ Snapshots are secured with different access credentials from other administrator credentials.

- ☐ Multifactor authorization can be deployed for all configurations.

- ☐ Snapshots can be tested prior to restoration to ensure they're free of malware.

"The cyber insurance application process we went through last year was quite extensive. The examiners came to our site and asked us numerous, detailed questions about our security policies and processes and how we performed and stored our backups. We told them we were backing up everything to the AWS cloud directly from our production filer. They were okay with that approach, but they preferred having a secondary filer taking care of the backups, not just our primary filer doing all the work. Going into this year's renegotiation for our policy renewal, we'll be in a much better place.

Cohesity is a well-known and trusted solution with the cyber insurance examiners. That's just another benefit I brought up when explaining the need for Cohesity to our executive team."

Arash Roudafshan, VP of Technology, Bardel Entertainment Inc.

"Not only did Cohesity enable us to safeguard our Exchange environment and move data management to the cloud, but we also easily meet the requirements for cybersecurity insurance."

Richard Humphreys, IT manager, The Southport School

"With Cohesity, we can answer 'yes' to new requirements for cybersecurity insurance—yes, we have immutable backups, keep a copy in the cloud, use MFA, and require multiple administrators to approve changes to backups.

Without those capabilities our insurance premiums would be much higher, if we could get insurance at all."

Matt Logan, CIO, Pearl River Community College

Cohesity can reduce
cyber insurance-related costs

According to Delinea, almost eight out of ten respondents (79%) said their insurance rates increased upon application or renewal, with over two-thirds (67%) reporting that they increased 50% to 100%.

Many Cohesity customers are happy to report they actually saw reduced costs related to their cyber insurance rates and premiums.

"Cyber insurance is not only harder to get, but premiums continue to dramatically rise. This year our premiums were set to double, while our coverage was going to be cut in half. We sat down with our policyholders and demonstrated the measures we take to protect our data, and how we will respond and be able to quickly recover with Cohesity. At the end of the conversation, we were able to cut our insurance premium costs by 35% and double our coverage."

Tim Fleming, director, Technology Services, Forsyth County Schools and co-author of Cyber Unboxed

"Using Cohesity immutable backups and ClamAV significantly lowered our premiums for ransomware insurance."

Christian Zinke, team lead for IT Infrastructure, Kassenärztliche Vereinigung Hessen

"With Cohesity we lowered TCO by 10-15% by decommissioning four legacy backup products, eliminating co-lo lease and equipment costs, and simplifying management. And ransomware protection helped us get favorable rates when we renewed our cybersecurity insurance."

Bobby LaFleur, officer of Information Technology, Spring ISD

COHESITY

Cohesity helps strengthen data, cyber, and business resilience

Because there's such a massive shift happening in how organizations secure and manage data in the era of multicloud and ransomware, it's important to focus not just on prevention, but on strong data, cyber, and overall business resilience.

Organizations that take this more modern, comprehensive approach—whether or not they ultimately opt for cyber insurance—are more likely to thrive if the rate of cyberattacks continues to accelerate.

"Just three days after the ransomware attack we had restored the majority of our manufacturing customer's operations, enough to resume production. The customer's cyber insurance provider said that other companies hit by the same targeted attack needed two to three weeks for even partial recovery. Fast recovery had a significant impact on the bottom line. Recovering in three days instead of the 14-21 days typical of this type of attack saved approximately $12 million in downtime costs. No ransom was paid. We give credit to our team—and to Cohesity."

Jesse Kegley, chief revenue officer, Emerge IT Solutions
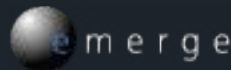
"Though we hadn't experienced a major cyberattack, we liked knowing that Cohesity's backups can't be altered by attackers, and that data is continually scanned to detect suspicious changes from one backup to the next."

Chris Dove, enterprise architect, California Department of Finance

"The immutable architecture from Cohesity ensures that our backup data can't be tampered with or maliciously deleted. Luckily, we've never experienced a ransomware attack, but with Cohesity, I feel very confident in our ability to detect and rapidly recover from any attack if something catastrophic ever occurred."

Shawn Robertson, platform manager, Acceptance Insurance
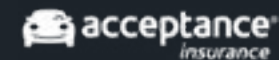
"The main reason we purchased Cohesity was for the added security it gives us with the immutable backups. We are happy with the Cohesity data protection solution. It is providing us with greater cyber resiliency and the peace of mind that comes from knowing everything's adequately protected and easily recoverable in an emergency."

Keven Denton, deputy CTO, West Ada School District

COHESITY

Ready to strengthen your cyber resilience?

Get to know our AI-powered data security
and management at cohesity.com