Data Backups

What are backups and why do they matter?

Backups are copies of a business' data. Cyber criminals often encrypt business data in a ransomware attack and demand payment for its release. Whether or not a business maintains proper backup often determines the most cost-effective resolution to a ransomware attack.

Recovering from a ransomware attack has become increasingly expensive in recent years, particularly due to lost income. In 2020, the average business interruption cost was $435,000[1] and the average ransom demand in Q4 was $154,000.[2]

Without backups, businesses pay $732,000 on average to restore data from scratch.[3]

How At-Bay helps keep businesses secure

We conduct a sophisticated security scan of every business we quote and ask whether they have set up segregated, offsite, or cloud backups. If a business has adequate backups in place, we offer full data restoration coverage, even for riskier classes looking for higher limits.

More than twice as many businesses impacted by ransomware were able to restore data from backups than those who paid the ransom.[4]

Backups are only effective if they are comprehensive and address all critical data, which is why businesses should audit all data locations to ensure no critical data is excluded from the backups.

Follow the 3-2-1 Rule

We recommend following the 3-2-1 Rule when creating data backups:

- Make 3 copies of the data.
- Store the data across 2 different mediums.
- Keep 1 copy of the data off-site.

To protect against ransomware, the offsite backup should be segregated from the business network.

---

[1] NetDiligence: Cyber Claims Study 2020 Report
[2] Coveware: Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demand
[3] Sophos: The State of Ransomware 2020
[4] Sophos: The State of Ransomware 2020