rubrik

74% OF ORGANIZATIONS STILL PAY THE RANSOM

HOW TO AVOID BECOMING A STATISTIC

When ransomware strikes, most organizations have no idea if their backups are clean, compromised, or even there at all, according to IDC research.

WHEN RANSOMWARE HITS...

25% didn't have backup or disaster recovery at all

25% had backups that weren't attacked (lucky, not good)

20% had backups targeted, but attackers failed to compromise them

30% had their backups successfully attacked and deleted

...YOUR LEGACY BACKUPS CAN'T HANG

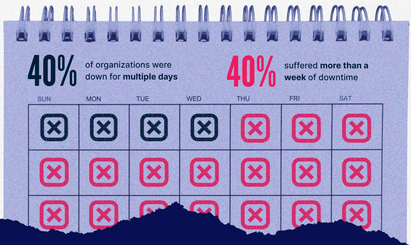
Organizations with intact backups face a brutal reality:

66% of ransomware victims experience data exfiltration

50% of those see sensitive, valuable date stolen

40% of organizations were down for **multiple days**

40% suffered **more than a week** of downtime



DON'T SETTLE

The IDC data shows that the majority of successful attacks exploited basic hygiene failures in backup environments.

39% didn't have air-gapped backups

28% lacked encryption for backup data

22% had no immutable backups

3 NON-NEGOTIABLES FOR RESILIENCE

The fastest cyber recovery time objectives aren't achieved during an attack, **they're built beforehand with:**

1 ABSOLUTE DATA SURVIVAL
modern backup solutions handles this

2 GUARANTEED DATA INTEGRITY
can you trust what you're restoring?

3 RAPID RECOVERY
how fast can you get back online?

Get the complete picture and see the data visualizations that make these numbers hit even harder.

Watch webinar

IDC, Forewarned Is Forearmed: Lessons Learned From Cyber-Recovery Research, Doc # US51952724, March 2024