Surviving ransomware: Data protection insights and strategies

ESG conducted a ransomware study for the second time in early 2023 (2023 Ransomware preparedness: Lighting the Way to Readiness and Mitigation) surveying 600 enterprise IT and cybersecurity professionals across North America and Western Europe. On 28 November 2023, Keepit and ESG organized an industry webinar to discuss the findings of the report. The webinar panel included Pavul Robichaux, Microsoft MVP and Keepit's Senior Director of Product Management, Dave Gruber, Principal Cybersecurity Analyst, ESG and Christophe Bertrand, Practice Director, ESG.

The report found that ransomware attacks are becoming so prevalent that it's a matter of when, not if.

- 75% of organizations had a successful ransomware attack in the last 12 months.
- 16% of organizations experienced a ransomware attack on a weekly basis.

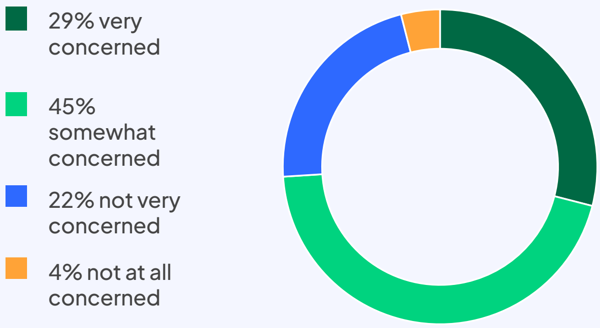
What is being affected by ransomware attacks?

The study found that the top target areas for attackers include key core IT infrastructure, storage systems, network connectivity, messaging and collaboration infrastructure, and identity and access. Cloud-based data is an increasingly popular target for ransomware attacks as well as the data protection infrastructure and mechanisms themselves.

Backups are a key target for ransomware attacks as victims will be more likely to pay the ransom if their ability to recover data is affected. However, there's no guarantee that all your data will be recovered after a successful ransomware attack. The ESG study showed that only 16% of respondents were able to recover 100% of their lost data.

Backups are a key target

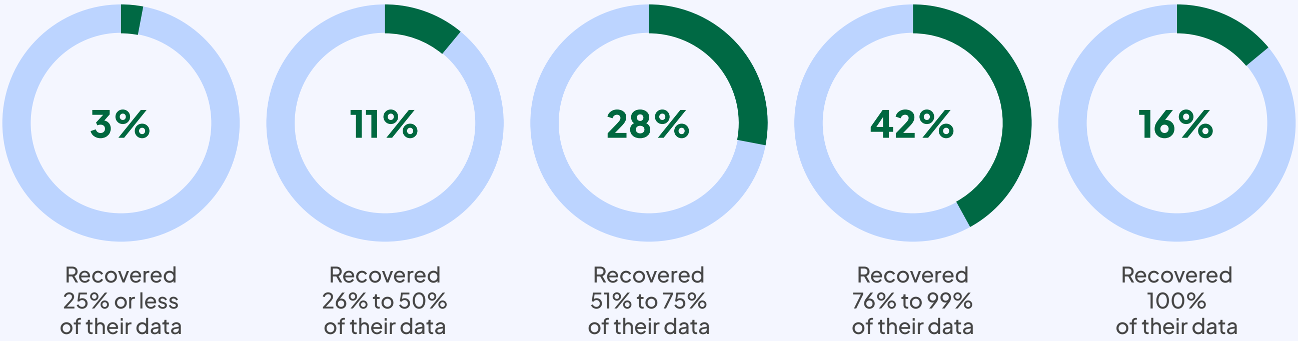
Level of concern that data protection copies could also become infected or corrupted by ransomware attacks



Nearly one in three express serious concerns about the security of their backups

Typically, not all data is recovered

Percentage of data organizations were able to recover



Key terms

Air gapping gives you a level of protection that makes your backup somewhat tamper proof. It means disconnecting the backup copies from mainstream production – ensuring they don't share the same risk profile.

Immutability means your data source can't be tampered with nor deleted.

How to build security strategies that protect from ransomware attacks?

1. Invest in preventative security controls. For example, network security, endpoint security, backup and disaster recovery infrastructure security and e-mail security are great places to start.
2. Test your capabilities continuously, including your recovery operations. This also helps you to understand what data is mission critical for your company and what the sequence is to recover lost data.
3. Be confident in your disaster recovery plans, including the immutability of your backup data. A good disaster recovery plan is jointly prepared within the company to ensure all sides of data protection and cyber security are considered.

Only 40% organizations said they take extra measures to protect all of their backups.

“The research showed that very few people had the ability to recover 100% of mission critical data. “

What does a winning ransomware recovery and data protection strategy look like?

Data protection checklist

- ✓ 100% of your mission-critical data is protected.
- ✓ Your backups are immutable and tamper-proof.
- ✓ Your backups are stored on a separate, air-gapped infrastructure.
- ✓ You regularly test and verify your recovery processes.

Evaluate your current ransomware recovery plan and data protection strategy

- ✓ How do you score on the data protection checklist?
- ✓ How much of your mission-critical data are you confident you can recover
- ✓ Are there additional steps you can take to improve your resilience and strengthen your last line of defense?

Here in Keepit we:

Are a completely independent backup provider with no dependencies on any public cloud. Vendor independence means you'll always have access to your data, even when disaster strikes

Deploy leading security measures, such as air gapping, immutability, and encryption both in transfer and at rest

Store data in seven regions, in data centers that don't have any shared components with any public cloud provider

Are ISO/IEC 27001:2013 certified – the entire company and all locations

Continue the conversation

Watch the webinar now on demand

Watch it now

Read the ESG report