FLEXENTIAL

5 Steps to Protect Against and Recover From Ransomware

Avoid payments by using smart backups

While malware, breaches, phishing and other cyberattacks have been on the rise for years, the dramatic explosion in ransomware attacks is shaking the IT security landscape.

By 2025, **at least 75% of IT organizations** will face one or more attacks[1]

Only **8% of organizations** manage to recover all the data following a ransomware attack[2]

Backups can protect your IT infrastructure against ransomware attacks and help avoid ransom payments by providing fast recovery of data, systems and applications.

Here are five steps to ensure a reliable backup and recovery strategy:

1. **Backup everything**

   It's only possible to recover what's backed up, and often not all data and systems locations are known by IT. Conduct a thorough inventory of systems and assets to identify all that needs to be protected.

2. **Keep the backups isolated**

   To protect against ransomware, at least one backup copy must be placed outside of your organization's building. It can be a second physical site or in the cloud. The off-site backup should be isolated from the business network.

3. **Build a tiered backup process to speed recovery**

   Classify your infrastructure in tiers according to sensitivity to downtime and business impact. The data, systems and applications that cannot afford a long period of downtime and data loss are your mission-critical infrastructure and should be protected accordingly.

4. **Keep the backup infrastructure up to date**

   As media decays and storage technologies evolve over time, critical enterprise data can become inaccessible during a ransomware attack. That's why it's essential to keep important backups compatible and available by periodically modernizing enterprise backup technologies.

5. **Test, test and test again**

   To know that you will be able to restore the data quickly, you must fully test the recovery process. If you don't test your backups and the recovery process, you won't know if it will work when you need it.

Smart backups and recovery strategies that utilize cloud-based infrastructure are a reliable, secure and cost-effective solution against ransomware attacks.

Choose the right backup and recovery strategy for your IT environment

For mission-critical IT infrastructure:
Disaster Recovery as a Service (DRaaS)

DRaaS is a cloud-based disaster recovery solution that replicates your IT infrastructure to the cloud in near real time. It protects the mission-critical environment that requires low RTOs and RPOs. DRaaS is secure, scalable and doesn't require upfront costs.

For non-critical IT infrastructure:
Backup as a Service (BaaS)

BaaS is a cloud-based backup solution that replicates data and applications to a safe and cost-effective cloud environment using a scheduled routine so that it can be retrieved on-demand. BaaS is best for compliance and regulatory purposes and non-critical infrastructure that is less sensitive to downtime.

By adopting a reliable backup and recovery strategy, you will have the confidence to provide business continuity and avoid the huge cost of payments and brand damage if a ransomware attack occurs.

Learn how Flexential can help you develop a robust backup and recovery strategy to protect your organization against ransomware attacks.

To learn more about Disaster Recovery Solutions click below:

LEARN MORE

Sources:
(1) Gartner.com
(2) Gartner.com