Disaster recovery checklist

Ransomware will happen—are you prepared?

Roughly every 21 seconds a new organization is hit by ransomware. With more than 4,000 attacks per day in the U.S., cyberattacks are not a matter of if but when. Ransomware costs businesses on average $1.85 million per incident. With these high stakes, organizations need to know how well they can respond to ransomware and other disasters. Review this checklist with your technical and business management teams to ensure the organization can fully and quickly recover.

Score these questions on a scale of 1 (not able to meet/support the requirement) to 5 (fully able to meet/support the requirement) to evaluate the disaster recovery process.

Key data recovery requirements	Score
Does top-level management fully accept and support the recovery plan? Recovery plans are often just solutions at a department level that serve a functional purpose, such as meeting an audit or compliance requirement. If the plan doesn't have support from the top-level business management team, the plan is often not comprehensive enough to be used in the event of a real emergency.	0
Is the company able to work after and even during a disaster? Traditionally, organizations used magnetic tape recordings for backup. But fully recovering from a tape can take an extended period. The backup tape needs to be shipped and environments rebuilt. Sometimes this rebuild can take days or weeks. This is not a process built for recovering a mission-critical application. And some newer storage-based solutions are often vendor dependent and force you to lock into a specific solution. However, today the industry offers modern vendor-agnostic solutions that deliver consistent recovery and flexibility along with reduced operation costs.	0
Does the recovery technology meet the business expectations of your organization? Some solutions only meet part of an organization's recovery goals or objectives. Many businesses need a solution with recovery point objectives (RPO)* of seconds and recovery time objectives (RTO)* of minutes that can be executed without impacting other systems. Restores from traditional recovery solutions can have an RPO of 24 hours and an RTO of days and require significant resources. Can your business tolerate impacts to productivity for that long? **RPO is the maximum amount of data – as measured by time – that can be lost after a recovery from a disaster or failure.* **RTO is the maximum amount of downtime a company can bear after failure.*	0

c spire business

Key data recovery requirements	Score
Are you using a single solution to meet all your recovery goals? Multiple solutions cause confusion and complexity during an actual disaster event. The right people need to be available with different specialties and with multiple DR tools. Sometimes these multiple people are not actually multiple people, but a single person with many roles. An effective solution should be very easy to use and automate as much of the process as possible. The goal should be to have one solution so that others without specialized skills can use it and execute the failover.	0
Is recovery and protection possible at the application level? Application groups ensure that all the virtual machines (VMs) supporting a mission-critical application are protected consistently and are in sync. This is especially important in environments with multiple servers and/or multiple databases for a single application. If the DR solution cannot effectively support application groups, ad hoc groupings can cause errors, especially in high pressure situations.	0
Can you recover VMs and restore application availability in near real-time? A true modern-day recovery solution will deliver continuous protection replication in real-time at multiple locations. As a result, the data is already at the recovery site, and restoration can start immediately. Also, a modern solution will perform non-disruptive testing at the replicated site without interrupting production activity.	0
Does the recovery team have the training necessary to fail over a site? Recovering from a disaster is not something you want to go into without relevant knowledge and experience of the environment. Often the technical components require testing and coordination. Specific items may need to be recovered in specific order for proper functionality or optimum recovery. **Training should include:** • Repeated and regular non-disruptive testing. • Longer-term testing in isolated environments to determine functionality. • Staff at the recovery site who can perform the failover in case something prevents the team from the primary site from participating in the recovery effort.	0

A score below 22 means the business is likely not prepared to fully and quickly recover from a ransomware.

Contact C Spire Business for help filling the gaps.

Total Score

0

START NOW