Tectrade
A CSI GROUP COMPANY

Data Protection

How to Assess the State of Your Data Protection Strategy

Just minutes of downtime can significantly impact your business.

Having a reliable backup and recovery strategy is essential to keeping your business up and running.

An outage can deliver a damaging blow to your company's finances and reputation with the average hourly cost of downtime cited by Gartner at $5,600 per minute[1].

The risks of this are increasing when you consider the high likelihood of downtime that could be caused by Ransomware attacks. The impact of ransomware on small to mid-sized businesses can be crippling. According to Malwarebytes among small to mid-sized organizations that have experienced a successful infiltration of the corporate network by ransomware, 20 percent reported that they had to cease business operations immediately, and 12 percent lost revenue, both slightly lower than the global average.

Recent surveys on IT spend show that only 7% of an organisations IT budget is spent on backup and recovery. This is a very small amount considering its importance in keeping a business up and running. It is therefore important to make sure that a business is making the most out of the budget they have for backup and recovery.

Taking stock of your approach to backup and recovery will help you correct mistakes so you can respond quickly to an outage and reduce costly downtime.

Tectrade have produced a checklist that can help you prepare for an outage:

Backup Frequency:

If data isn't being backed up continuously, you will risk losing valuable information.

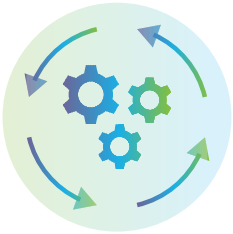
- Do you have automated backup?
- Are your backups scheduled as requently as required to meet your recovery objectives
- If you use tape backup, do you move them offsite as frequently as you back up to them?

Backup and Recovery Testing:

Don't wait until an outage occurs to find out whether your data protection strategy works.

- How often do you test backup and recovery?
- Are you able to identify critical systems that would require fast recovery in the event of outage or ransomware attack?
- Do you test backup and recovery in real-world scenarios?
- Are you able to test backup and recovery without disrupting production?

1 https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/



RTO and RPO Goals:

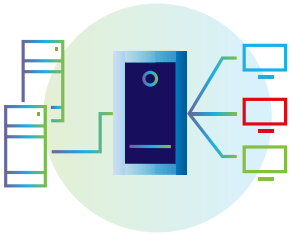
Data needs to be recovered quickly and with minimum loss or compromise.

- Are you able to meet your recovery point objectives (RPOs) and recovery time objectives (RTOs)?
- How much downtime can your business tolerate?
- Are your RPOs and RTOs realistic?
- Are your RPOs and RTOs measured in hours, minutes, or seconds?

Backup Capacity:

As data growth accelerates, finding space for backup copies of data becomes more challenging.

- Are you confident that your storage can handle the amount of data you need to back up?
- Can your backup scale to meet data growth demands even in the petabyte storage era?
- Does your data protection solution include cost and space-saving data management tools?



Supporting Infrastructure:

Your backup and recovery is only as effective as your IT environment allows.

- Are you working with legacy hardware and software that has lost vendor support?
- Have you considered how migration to the cloud will affect your backup strategy?
- Do you have resources for off-site backup?
- How much visibility do you have into your backup?
- Do you receive alerts when backups fail?
- How many tools do you use for data protection?
- Is your cyber defense strategy working in partnership with your backup and recovery strategy?

If you are unable to answer these questions and would like to know how well your data protection will work during an emergency. Tectrade can help with by conducting a full audit.

Don't wait for ransomware or an outage to strike, make sure your backup and recovery is the best it can be. Contact Tectrade today.

Get in touch:
info@tectrade.com

US
379 West Broadway
New York, NY 10012
+1 646 493 9811
www.us.tectrade.com