INSIGHTS PAPER

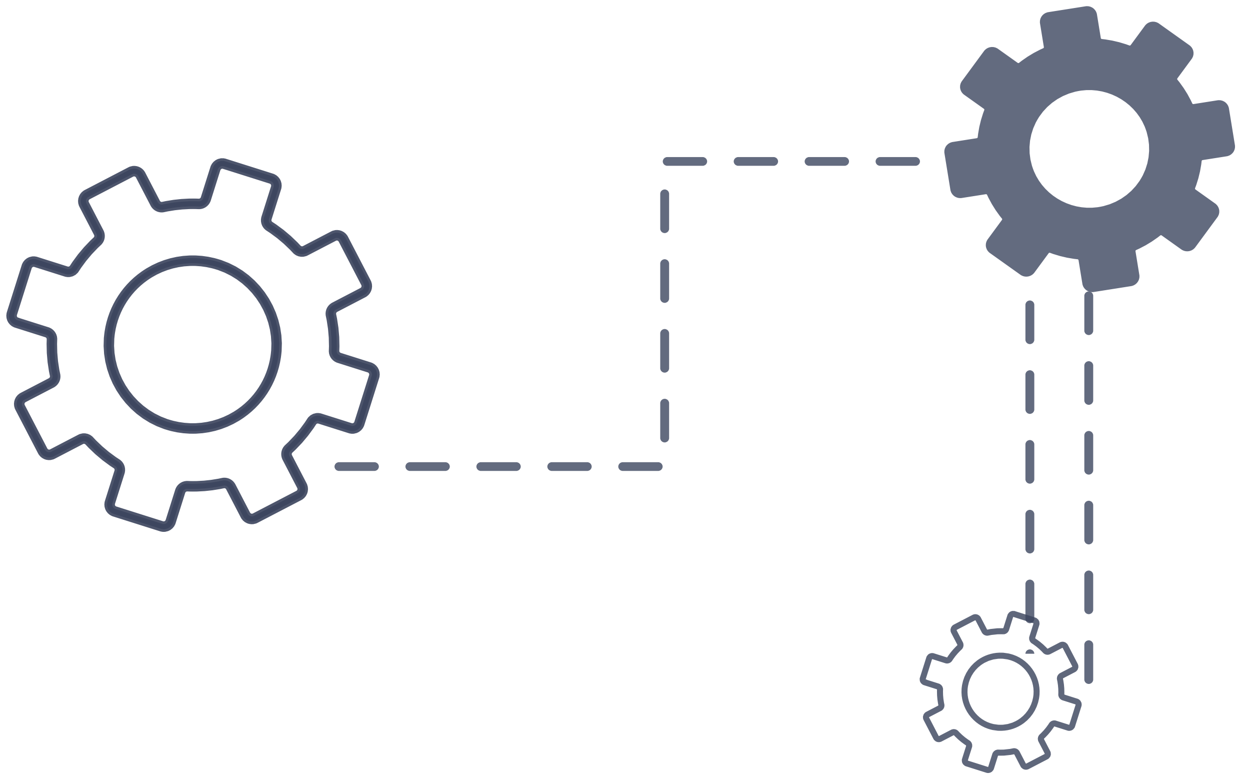
Are You Confident You Can Quickly Recover From a Data Disaster?

If Not, Ask The RIGHT Questions

PAUL HAGEN

If you are responsible for data security in your organization, you've likely had recent interactions with your IT group around recovery time and recovery point objectives (RTO and RPO). You want to know if your data assets are safe and recoverable, not only from traditional data center gremlins, but also from emerging and increasingly sophisticated cyber threats, particularly ransomware..

WHAT DOES RECOVERY LOOK LIKE?



Mission critical workloads are becoming increasingly distributed, both physically and logically. The data that underpins these workloads is extremely valuable to an organization. Sure, you still may need physical hardware, operating systems, microservices, APIs, and applications working together to present the data as useful information, but it is the integrity of your data that you are most concerned with when hit with the big ‘R’.

Let’s say you’ve already gone through a business impact analysis (BIA), established a business continuity plan (BCP), and derived from it a disaster recovery plan (DR). You also know IT has a playbook that is ready to activate when the inevitable hits. Great start! You can use those artifacts to meet regulatory, insurance, and compliance requirements and, as a bonus, they can even assist with a structured approach to address common data disaster scenarios.

WHAT DOES RECOVERY LOOK LIKE?

What many of these activities don’t do is ask a couple of really key questions:

1) Can you actually recover your digital assets within the SLAs that were set? How long will it take?

2) Can you assess quickly how much of your data is compromised?

The answers to these questions most likely live with your operations teams – if you haven’t asked them lately you should. The bottom line is that your ability to recover successfully could be dicey at best, and it may be because you haven’t asked the right questions of the right people.

I wanted to share a few additional questions that I think are critical to really understanding how well-positioned your organization is to respond to a Ransomware attack. While not necessarily an exhaustive list, these are a good place to start to give you a sense of where you stand.

Questions For The Business

- Do we have a regularly reviewed:
  - Business Continuity Plan?
  - Disaster Recovery Plan?
  - Business Impact Analysis/Risk Analysis Assessment?

- Do we have adequate cybersecurity insurance?

- Do we consider paying a ransom?
  - Do we have quick access to cryptocurrency to pay the cybercriminals?
  - Do we retain a negotiator as a middleman?
  - Can we accept sensitive data exposure and potential publishing of compromised sensitive data?

Questions For IT

- Do we have defenses that can baseline normal behaviour, detect unusual changes in data, and alert you in real time?

- Do we have visual insights that will accurately identify the extent of the compromised data and impact of an attack?

- Are our backups immutable and in a stored format that is write-once, read-many?

- Can we confidently recover the ‘specific’ data that was compromised, within RTO and RPO SLAs, while keeping our non-exposed mission critical workloads running?

- Have we run through tabletop exercises for mock data recovery?

Are You Confident You Can Quickly Recover From a Data Disaster?
If Not, Ask the RIGHT Questions

Each of these questions needs to be asked, and then mapped to a possible outcome that outlines what you need to do should an unexpected scenario arise.

For the record, we do not recommend any company establish a strategy of paying the cybercriminal because it proliferates the ransomware 'business' and makes it stronger. It also shows you are willing to pay which can make you a recurring target.

If you find the answers to the remaining questions stated above are anything but 'Yes, absolutely, let me show you' then you have reason to believe you need to shore-up your defenses.

You may want to redefine and review your 'people and processes' and continue doing that on a regularly cadence. Equally important is to find the right tools and technology, like Rubrik's Polaris Radar, to enable you to recover quickly and accurately to match your RTO and RPO SLAs.

Being able to recover from Ransomware is not the same as having a Ransomware plan.

WHERE TO GO FROM HERE?

Please reach out to us if you are interested in learning more about technologies like Rubrik, that don't just back up your data, but protect it and allow you to reduce recovery time from days and weeks to hours or less.

If you have concerns about your overall Ransomware preparedness, I'd encourage you to connect with our Risk, Security and Privacy team who can more fully assess your current position and provide recommendations for where to start.

Check out our our Ransomware Readiness Assessment.

About Paul Hagen

As Online's Director, Infrastructure Services Paul oversees Online's infrastructure team and supports a number of Online's clients.

online

To learn more about how Online Business Systems can help your business,

visit obsglobal.com