Data Backup: #FAIL

Put your processes and technology to the test

r² rack squared

expertise, technology, environment

Your business runs on IT

At the core of IT is your company's data, which may be your most valuable asset. Unfortunately, many companies' data backup strategies fall short, leaving their businesses at risk in the event of accidental loss, hardware failure, disaster or even malicious attack.

Think about the information you need to keep your business up and running. You have current and historical financial information, customer account information, manufacturing and inventory data, vendor information and, in many cases, governance and compliance data. **Can you afford to lose any of your data?**

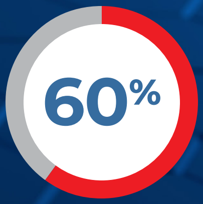
For most companies, data backup is viewed as a necessary evil. Something you would not dare overlook, but also something that probably doesn't get the level of attention and scrutiny it deserves. Budget constraints limit what IT can do in terms of backups, and a lack of experience and expertise can hamper your ability to develop a holistic backup strategy.

How confident are you that your backup strategy would allow you to recover in an emergency?

Your company's future could hinge on the completeness of your backup strategy.

Most companies don't realize that their current backup strategies are incomplete. The problem is they discover the gaps far too late—when they can't recover from an incident.

This guide examines the most common pitfalls in backup strategies. Its questions can help you take a closer look at your own backup strategy and identify where you may need to make improvements.



Data loss happens. Over the course of a year, 60% of small and medium-sized businesses experience loss or theft of sensitive data.

—*Ponemon Institute*

5 questions to put your backup strategy to the test:

1 Do you have a comprehensive backup strategy?

2 Is your backup technology outdated?

3 Are your backup copies properly secured?

4 Does your backup strategy include regular testing?

5 Are you assuming your cloud application data is being backed up?

QUESTION #1:

Do you have a comprehensive backup strategy?

To make sure your backup strategy is complete, consider your why, when, what, who and where.

Why perform backups? In the event of an incident that causes data loss, your business needs to recover using a good data backup that can keep the company up and running.

When and how often do you back up? Backup frequency matters. If it's not frequent enough, you are at risk of losing valuable data. But backing up too often can lead to greater expense for storage and data management. You need to consider how dynamic your data is and make sure backup intervals reflect that.

What data do you back up? How dynamic is your data and where it is located? Have you considered when you need a full backup vs. incremental or differential? Have you accounted for data that is in the cloud or do you just assume it is backed up? What about software applications? Are you only focused on the data files or are you backing up the applications? These are just a few of the questions you need to consider when designing your backup strategy.

Who is responsible for backups? Backups are typically a side job for an individual, and if that individual is out of the office, the backup process is not executed or monitored. This process needs to be viewed as a critical part of your IT strategy, with a primary and secondary person who understand their roles and the importance of the backup process.

Where are your data backups? Backing up your data and then storing it in the same physical or logical location as your primary data is a recipe for disaster. A solid backup strategy calls for keeping at least one copy in a secure location off-site.

A cloud backup services provider knows the right answer to all these questions and can develop a solution to meet the unique needs of your business.

Understanding the "3-2-1 best practice" for backups:

3 copies of data,

2 different media types,

1 copy held off-site.

QUESTION #2:

Is your backup technology outdated?

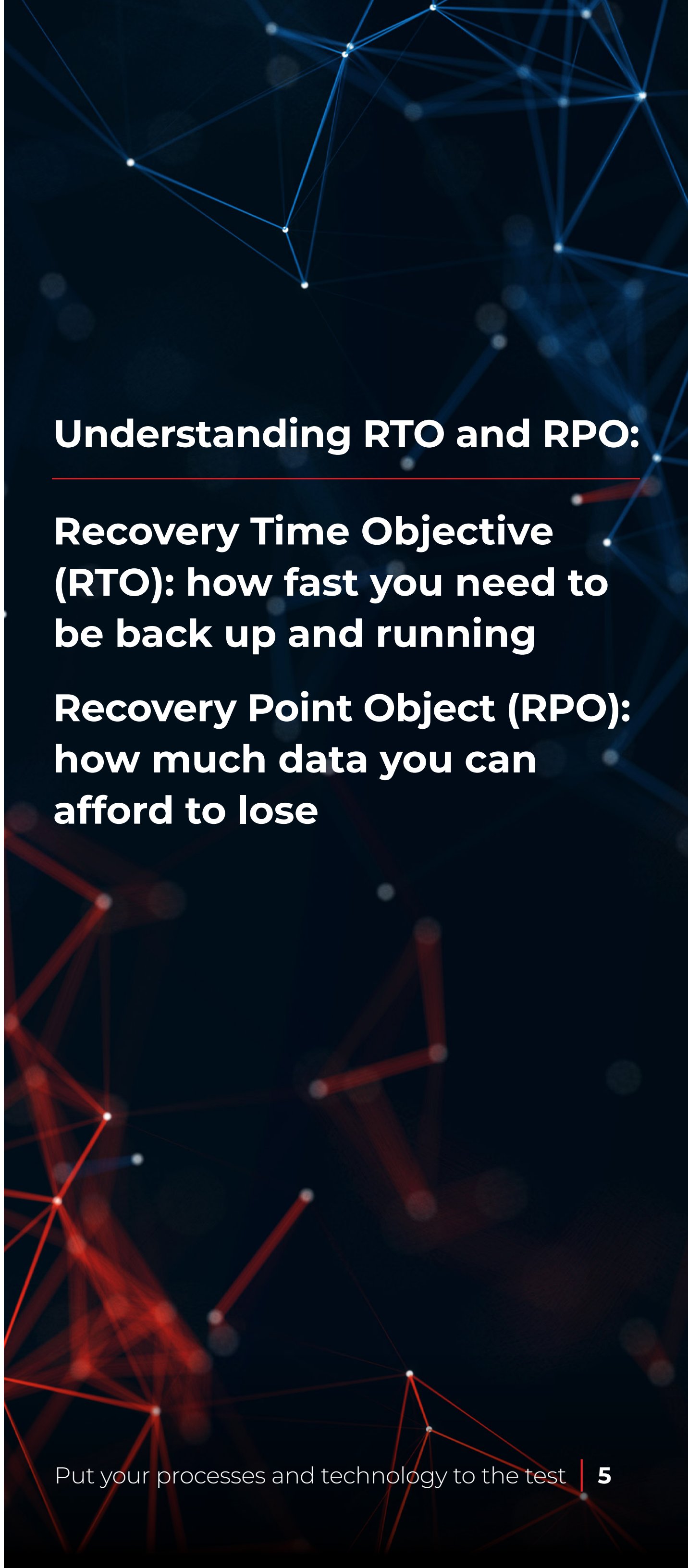
Technology changes fast, and backup technology is no different, but many companies take the “if it’s not broke, don’t fix it” approach to their backup systems. This can be a mistake as, due to the nature of backups, you might not know the technology is “broken” until it’s too late.

There are several things that can go wrong with old technology.

- Security technology continues to evolve, but if you don’t upgrade your backup system, you could find yourself encrypting and storing data with old methodologies, possibly leaving you out of compliance with company, industry and government standards.
- As you upgrade your hardware and software, older backup technology may not be compatible with the new. This can lead to companies supporting multiple backup solutions and technologies to backup all devices.
- And let’s not forget your data in the cloud. With more applications moving to the cloud, it is important that you have the ability to backup both your onsite data and your data that is stored in the cloud. Many older technologies do not support cloud backups.

Your backup technology’s capability is important to consider when calculating your RTO and RPO. Newer technologies are going to be more efficient, allowing you to reduce these numbers.

A cloud backup services provider performs backups as part of their core business, which means they are constantly investing and upgrading to the latest technologies.



Understanding RTO and RPO:

Recovery Time Objective (RTO): how fast you need to be back up and running

Recovery Point Object (RPO): how much data you can afford to lose

QUESTION #3:

Are your backup copies properly secured?

For many companies, IT gets squeezed into an out-of-the-way office, spare closet or extra space in the warehouse, falling short of providing a safe, secure environment for the equipment and data. The “best available” space is designated for primary computer equipment, leaving “next best” for storing backups.

Take care of these key concerns to be sure your backups are safe and secure.

- **Protect against fire:** For backups that are stored on-site, be sure to store media where it is protected from fire or extreme heat. Storage media are more sensitive to heat than some other items and may not be safe in a fireproof room or in a safe designed for document storage.
- **Be geographically distanced:** Carrying tapes to another building on the same campus is better than being in the same building, but may not protect you in the event of a natural disaster that damages the entire location.
- **Secure copy off-site:** Consider how you will get one copy off-site so that data is going directly to a secure location versus being carried around by an employee, creating the opportunity for it to be lost, stolen or damaged.
- **Break the physical and logical connection:** Backing up to a remote device can be a great solution, provided you take the right security measures. A remote device on the same logical network is easy prey for a hacker that is lurking and learning.

A cloud backup services provider addresses all of these issues so you know your backup data is secure.

QUESTION #4:

Does your backup strategy include regular testing?

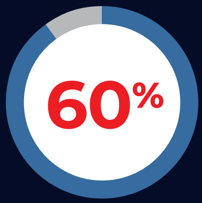
Having a solid data backup strategy in place is like an insurance policy for your business. You want to have a good policy, but you hope you never have to use it. Because you rarely access your backed-up data, it's easy to assume everything will work as planned.

But assuming that your backup process is running smoothly, rather than verifying it, is a recipe for disaster. When you need your backup data is not the time to be figuring things out. Here are some steps you can take to make sure you are prepared for an incident:

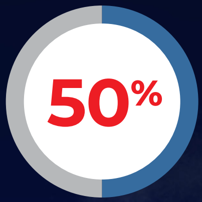
- **Create a "playbook" for restoration that details how to execute the process.** Then practice. In the event of a disruption, this playbook calls out what files have been included (or excluded) and the order of operations for restoring files. Practice runs will help you avoid the confusion of figuring out data recovery on the fly and give you a good sense for your actual recovery time.
- **Schedule regular checks to be sure your backups function as they should.** Companies typically perform backups at night with an unmonitored process. If they fail, it is not discovered until the next day and if not corrected will repeat itself during future backups. By performing regular checks of backups, you can identify issues and address them proactively.
- **Recover your backup on a device different than your production hardware.** Don't assume that your failure will simply be lost data. Assume a catastrophic hardware failure that requires you to recover data on another device. Then take the time to recover to the backup hardware and confirm it is compatible with your data backup.

A cloud backup services provider can work with you to develop a process for testing backup and recovery procedures so you can be confident in your ability to recover if needed.

According to Ontech.com,



of backups are incomplete, and



of restores fail.

QUESTION #5:

Are you assuming your cloud application data is being backed up?

Over the last 10 years, there has been a major shift away from on-site applications to cloud-based SaaS solutions. These solutions offer many benefits to companies, but there is some confusion in the market about their responsibility for your company data.

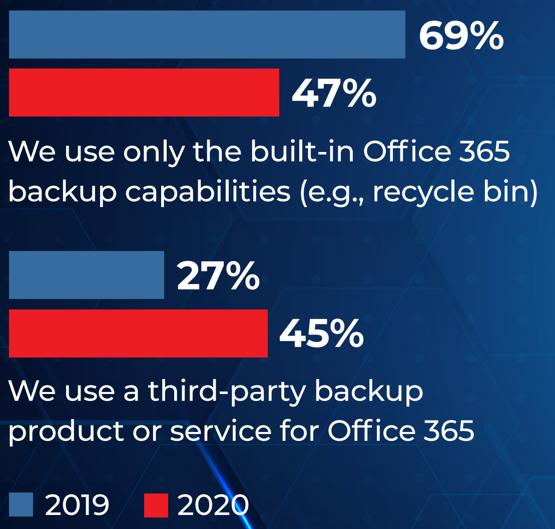
SaaS solutions are designed with resiliency in mind. You never have to worry about whether your email (O365), CRM, ERP or other strategic business application is up and running. The same does not hold true when it comes to the availability of your data.

The misconception about SaaS is that not only is the application always available, but people assume that their business data is being backed up along with the application. The fact is, most SaaS providers are not backing up your data. This means that if you accidentally delete a file or if something happens on the SaaS provider's end and they lose your data, there is no recovery and no recourse.

Knowing how important your data is, some SaaS providers offer data backup as an option. This might sound promising, but often they charge high fees to recover lost or missing data. Your best bet for protecting your data is to implement a backup solution of your own.

A cloud backup services provider can work with you to evaluate the cloud-based applications you are using and identify the best option for backing up your data.

Office 365 is on the rise



Why Racksquared?

We deliver “3-2-1 best practice” backup solutions in the cloud, while you focus on your core business. How do we do it?

EXPERTISE

Racksquared has engineers and system admins who specialize in developing and executing backup strategies designed to keep businesses up and running. This team manages, monitors and supports our customers’ data backups around the clock.

TECHNOLOGY

Racksquared leverages the latest technologies, including storage area networks (SANs), virtual tape libraries (VTLs) and backup software from industry-leading providers. This means our customers’ backups and restores are fast, reliable and meet their established RTOs and RPOs.

INFRASTRUCTURE

Racksquared’s data centers and network are designed to be secure, reliable and resilient so that our customers know their data backups are working properly and are readily available when they need them.

CASE STUDY

Backup and recovery technology protects The Columbus Zoo and Aquarium from the potential of data loss.

CHALLENGE:

With a limited IT staff supporting a wide range of business needs, The Columbus Zoo and Aquarium was looking for a secure off-site location to back up business-critical data. With a tight budget to work with, investing in an off-site location of their own and purchasing new technology wasn't an option.

SOLUTION:

They turned to Racksquared, which was already providing them with colocation services, to look at options. Racksquared implemented a Veeam cloud backup solution that ensures all their data is backed up daily and is readily available if they need to restore it.

RESULTS:

The Columbus Zoo and Aquarium now has a data backup and recovery solution as well as a disaster recovery solution that they know they can count on should they ever need it. Benefits include:

- Access to IT expertise and consultation when they need it
- The advantage of the cloud business model in which they only pay for what they use
- Leveraging secure off-site data backup with access to disaster recovery infrastructure

What our customers say

"With Racksquared, we now have best-in-class protection of our data, using the 3-2-1 backup model and the cloud data management solution has drastically reduced the manual efforts demanded of my team."

— Debbie McMasters, System Administrator, The Columbus Zoo and Aquarium

"Racksquared has worked with us to develop a data backup and recovery strategy that enables us to meet our specific Recovery Time Objective and Recovery Point Objective."

— Eric Wasserstrom, President, N. Wasserstrom

Get started today

Interested in learning more about backing up your data to the cloud?

LEARN MORE

Visit racksquared.com/Cloud-Backup-Solutions to learn about the backup solutions we have available to support your business needs:

- Veeam Cloud Connect backup solutions
- Cybernetics VTLs and replication solutions
- Colocation with backup solutions
- IBM Power Cloud backup solutions
- 3-2-1 backup best practice

SCHEDULE AN ASSESSMENT

Racksquared works with you to understand your business needs as well as your current backup strategy and processes. Visit racksquared.com/assessment for a holistic assessment that includes:

- Current environment—Review what you have in place and your underlying challenges
- Potential risks—Identify hardware and software that is not updated, out of support or approaching end-of-life
- Site audit—Evaluate the physical risks of your environment
- Backup system and processes—Understand how backups are performed and identify any gaps that should be addressed
- RTO and RPO—Determine if your current backup strategy will enable you to meet these objectives
- Disaster recovery—Review your systems and processes to evaluate your ability to recover in a timely manner

At the end of the assessment, we provide you with a summary of our findings as well as recommendations on the best approach for deploying solutions to meet your business needs.

CONTACT US

Our team of experts is available to work with you to understand your current backup strategy and processes, the challenges you are facing and how we can help address them.

Give us a call at (855) 380-7225 or email sales@racksquared.com.

Your business runs on IT.
Let Racksquared keep your business up and running.

r2 racksquared

expertise, technology, environment

Racksquared can help simplify IT so that you can focus on growing your core business and evolve to meet the changing demands of customers. We do this by providing access to technical expertise, the latest technologies and a secure, reliable, resilient environment for your IT systems. We become an extension of your team, providing flexible designs and solutions while managing, monitoring and supporting your infrastructure, so that your business is always up and running.