WHAT YOU NEED TO KNOW TO PREPARE FOR A DATA LOSS EVENT

A Comprehensive Guide to Data Backup and Recovery

Connection®
we solve IT®

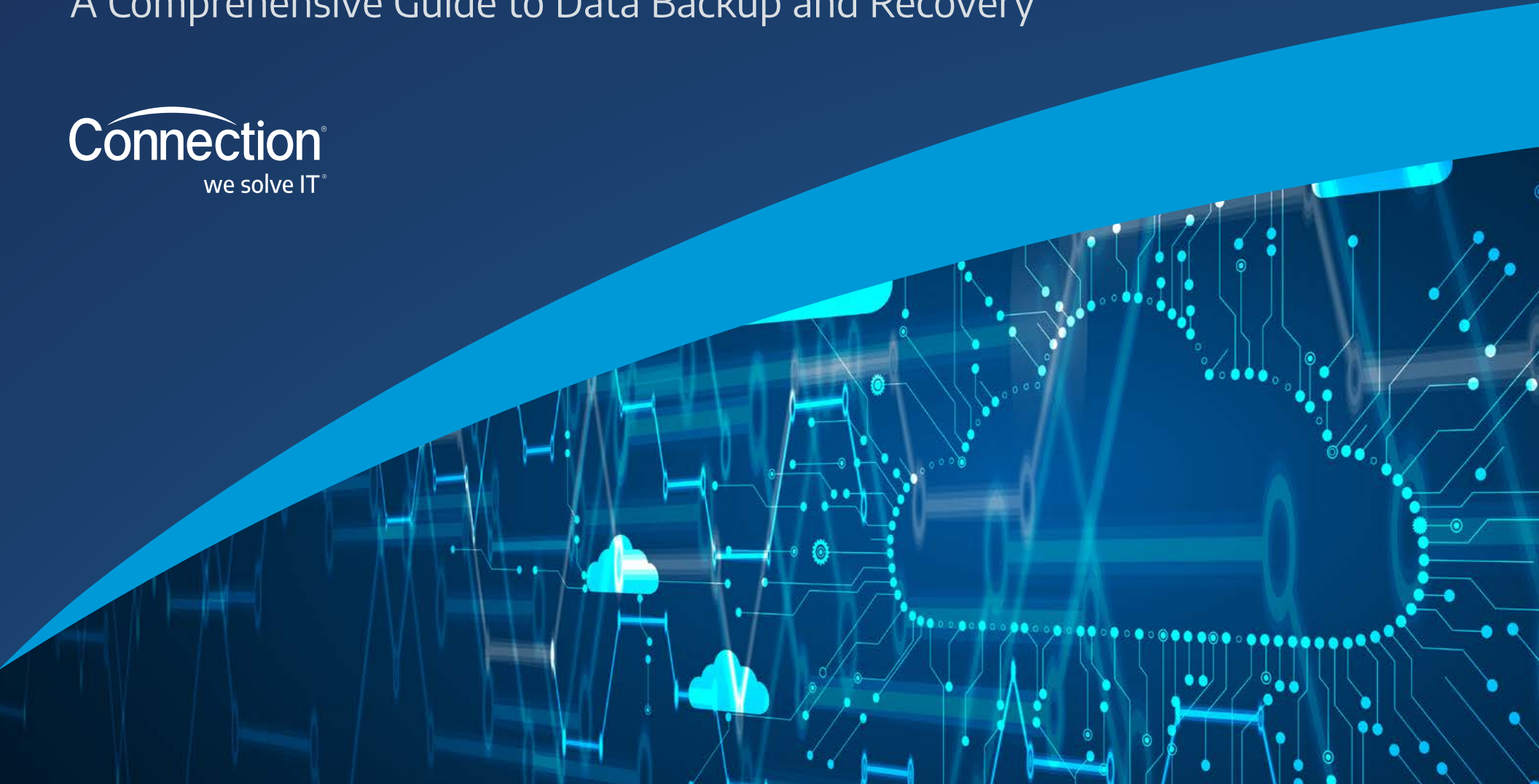


TABLE OF CONTENTS

INTRODUCTION

Today's organizations are constantly generating data that helps inform decision-making and facilitates operations and growth. Managing and protecting all that data can quickly become overwhelming. Backing up your digital data and establishing a recovery plan are essential steps in safeguarding a modern organization.

Prevention is essential, but incidents can happen even if you take all the right steps. Data loss can occur due to system failure, human error, power outages, natural disasters, intentional theft, viruses, ransomware, or other types of attacks. Many of these issues are relatively common, with IT leaders reporting that 28% of their servers had at least one outage during the past year.[1] And 93% of ransomware attacks also targeted backup data.[2]

Reliable backups of critical data are what will keep your organization running after an incident. The benefits of backing up data and having a plan for data recovery is that your organization:

- Safeguards data
- Protects work from disruption
- Secures continuity and productivity
- Ensures data recovery
- Minimizes the expense of recovery

Storage, backup, and recovery plans require time and monetary investments. However, the long-term benefits and peace of mind usually outweigh the initial effort. An hour of downtime costs most organizations of all sizes more than $300,000.[3] That's in addition to the cost of recovery and permanent data loss.

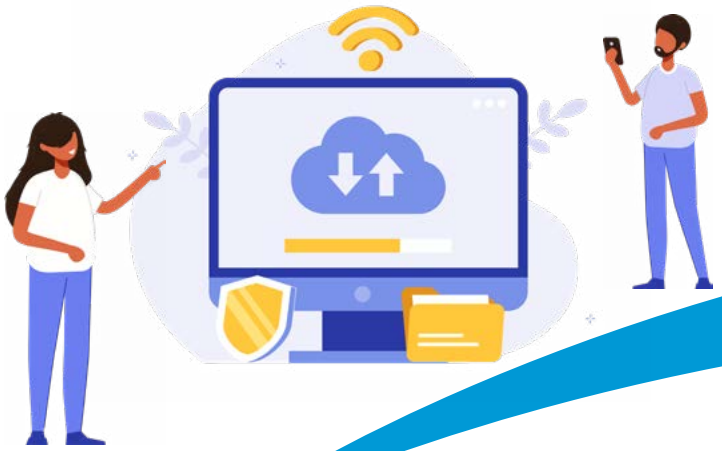
Unfortunately, many organizations underestimate the risks to their data. Forty-eight percent of executives and IT professionals said they aren't currently at risk.[4] However, once they reviewed a list of potential risk factors, 97% said they perceived risks to their organizations.[4]

CHOOSING YOUR METHOD OF DATA STORAGE AND BACKUP

Consider the types of data backup you'll need to perform full, incremental, or differential backups. A full backup is making a copy of all your files in one process. An incremental backup saves the new data generated since the last full or incremental backup. It is often performed daily or at other frequent intervals. A differential backup identifies all the files that have changed since the last backup and makes it easier to complete a full restoration.

A full backup copies all your data in one version, requires more storage, and takes longer to restore. However, when you lose data, it allows you to get back to working faster. Differential backups are easier to run and take less time to restore.

It often makes sense to use a combination of methods. If you're adding a lot of new data all the time, you may need to run full backups more frequently. If you're usually accessing data without making changes, you can rely more on incremental and differential backups. You should also factor in how much storage you have available and how much time you would be able to spend on recovery. In the case of complete data loss, you need the last full backup, the latest differential, and your incremental backups.

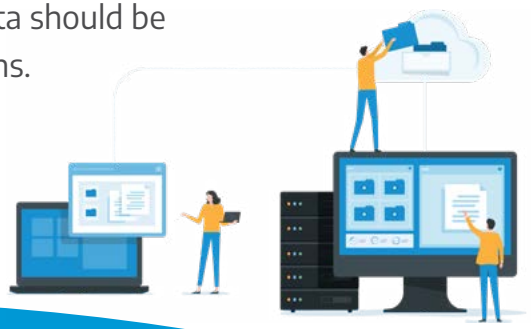


WHERE AND HOW TO BACKUP YOUR DATA

An effective backup and recovery plan starts by choosing the right methods and tools. You can save backup copies of your data using a combination of these methods:

- **On-premises:** Backups are stored using on-site devices. These include servers and external hard drives.
- **Cloud:** Private or public cloud services store backup data. Multi-cloud backup means using a combination of different cloud services.
- **Hybrid:** A combination of cloud and on-premises storage methods store backed-up data. Critical data is backed up using a variety of methods.

Cloud backup is valuable for protecting backup data from on-site disasters. But it can also be vulnerable to ransomware attacks or deletion. The most critical data should be backed up in multiple locations.



The 3-2-1 backup strategy recommends keeping three copies (original plus two) of your data in two formats or media types, including one copy offsite that is not connected to your network. One of the two duplicates should be immutable, meaning it does not allow data to be changed or deleted.

Currently, 90% of organizations use a mix of platforms for storage and backup. And 54% say their disaster response plan is to recover data on-premises, though most of the source data will come from cloud backups.[1]

GET STRATEGIC ABOUT DATA STORAGE AND BACKUP

Cloud and hosted services (including online backup and restore) are one of the top three spending categories for IT departments. However, some teams spend money on solutions without a consistent schedule or plan.[5]

Planning around data backup and recovery means considering what you need to do both before and after a data incident.

BEFORE DATA LOSS

The best way to minimize costs while protecting data is to be strategic in planning and designing backup and recovery plans before an incident occurs. Determine where and how to back up data. In case of a physical disaster, you'll want your data backed up in the cloud, not just on-premises. In case of a cyberattack, make sure your data is backed up offline so you can access it if an attacker gains control of your systems. For instance, in a ransomware attack, the criminal holds your data or systems hostage, demanding you pay them to be able to access your assets. Ransomware has been part of nearly 70% of the year's malware incidents.[6]

After deciding what you need to do to protect your data, you can begin to consolidate and migrate data. Start with identifying and prioritizing the most important files and systems.

GET STRATEGIC ABOUT DATA STORAGE AND BACKUP (CONTINUED)

AFTER AN INCIDENT

Prioritization will also help you create a recovery plan. Loss of data access can result in downtime and long-term consequences. If there is a data loss incident, do you know how to recover and restore your systems to where they should be?

To save time and productivity, it's best to have a plan in place. The average time to recover production data after a cyberattack is 24 days[7], so a recovery plan can help you get a jump start on getting back to business.

It's difficult to act in a crisis, so start by documenting the steps your teams will want to take. Define steps, responsibilities, and their owners, as well as timelines for recovery. You can update and add to it over time. Consider likely and even unlikely scenarios.

ANSWER QUESTIONS LIKE:

- Who is responsible for maintaining and updating recovery plans?
- Who initiates the recovery?
- Will internal or third-party resources conduct backups, assessments, and recovery?

Backup doesn't necessarily equal recovery. You may need to acquire backup hardware or decompress data and determine what you're missing. The actual transfer and restoration could be a lengthy process. You can minimize recovery times by sharing the plan with stakeholders. It also helps to identify and tier data and application backups by priority level. Higher priorities will require different kinds of backups as well as different timelines for getting back online. It pays to test your recovery and restoration plan regularly.

SETTING GOALS

When developing a backup and recovery strategy, keep these priorities in mind at every step:

Security of Data:

- Will data be encrypted?
- Are there ransomware protections?
- Do you have off-premises and immutable backup options?

Cost and Speed Efficiency:

- Are you paying for more storage than you need?
- Could a backup as a service (BaaS) provider save you money?
- Have you compressed and deduplicated your data?

Data Availability for Users:

- Have you established a backup schedule that doesn't interfere with work?

Data backup and recovery investments need to realistically align with your needs, objectives, and budget. Consider how you will balance the costs of downtime, disruption, and recovery with the costs of capital expenses, expert consulting, and cloud subscription costs.

FOLLOWING BACKUP AND RECOVERY BEST PRACTICES

When designing your plans, consider these best practices:

- Back up data multiple times a day and at regular intervals.[8]
- Perform testing on backup and recovery systems.
- Use more than one method for creating and storing backups.
- Use offline and offsite storage to ensure access.
- Encrypt backups to protect data.
- Set up devices and endpoints so work is on your servers or in the cloud.
- Work with an expert to ensure you don't have gaps in your plan.
- Use an immutable backup repository, which does not allow data to be altered or erased.

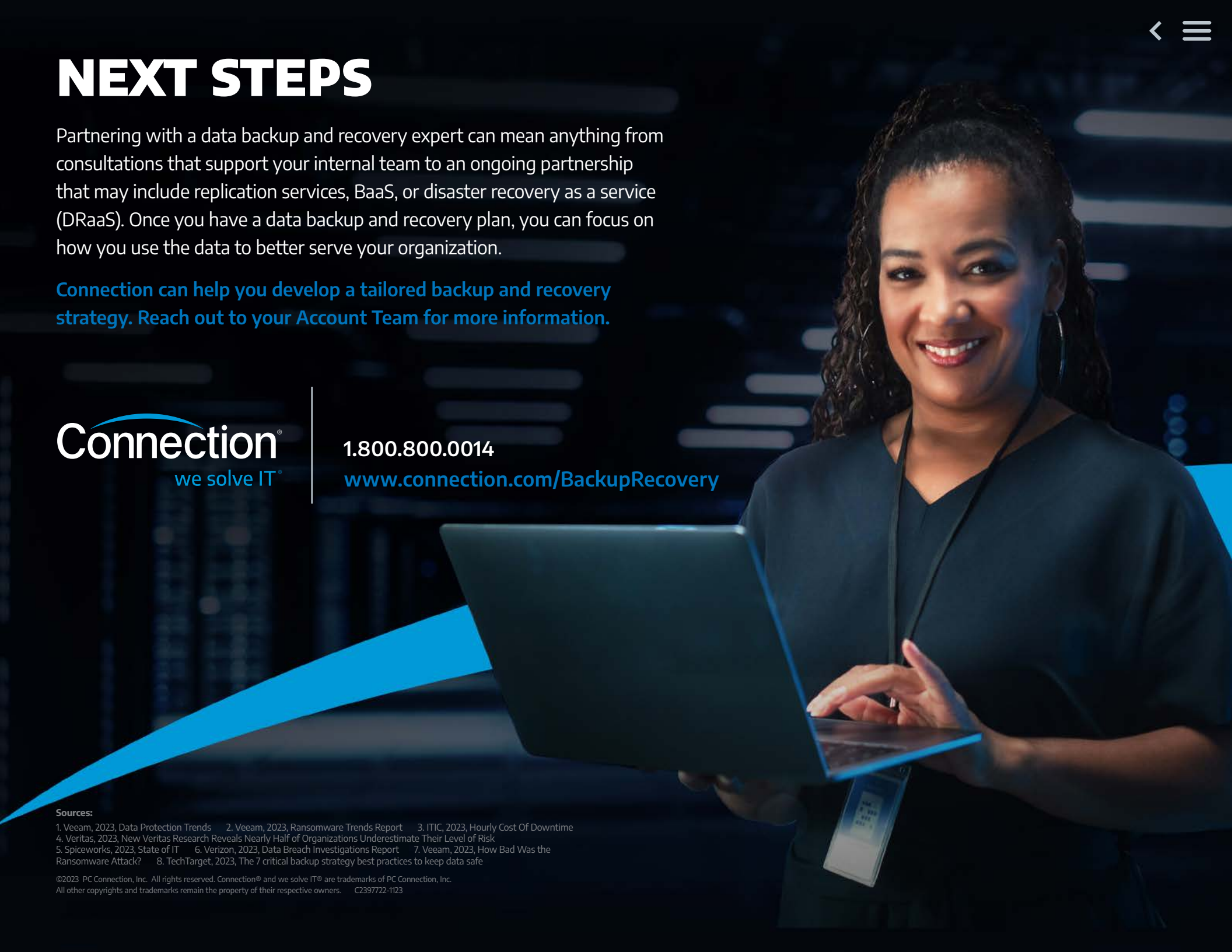
NEXT STEPS

Partnering with a data backup and recovery expert can mean anything from consultations that support your internal team to an ongoing partnership that may include replication services, BaaS, or disaster recovery as a service (DRaaS). Once you have a data backup and recovery plan, you can focus on how you use the data to better serve your organization.

Connection can help you develop a tailored backup and recovery strategy. Reach out to your Account Team for more information.

Connection®
we solve IT®

1.800.800.0014
www.connection.com/BackupRecovery



Sources:

1. Veeam, 2023, Data Protection Trends 2. Veeam, 2023, Ransomware Trends Report 3. ITIC, 2023, Hourly Cost Of Downtime 4. Veritas, 2023, New Veritas Research Reveals Nearly Half of Organizations Underestimate Their Level of Risk 5. Spiceworks, 2023, State of IT 6. Verizon, 2023, Data Breach Investigations Report 7. Veeam, 2023, How Bad Was the Ransomware Attack? 8. TechTarget, 2023, The 7 critical backup strategy best practices to keep data safe

Connection®

we solve IT®

1.800.800.0014 ■ www.connection.com