*A quick guide to*

# DATA RECOVERY

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

*See what your technology can do.*

www.visualedgeit.com

# Introduction

Today, data-driven decisions are helping businesses flourish. Analyzing data provides insight into a business's financial health, drives marketing decisions, and bridges the gap between expectations and reality. It enables companies to set clear benchmarks and work towards enhanced business efficiency and increased productivity. So, it's safe to assume that data is one of a company's most valuable assets. Among the most valuable data types for any company are IT data, customer data, and financial data.

In the same manner that a company focuses on the product supply chain or expanding warehouse locations, determining how to keep your data safe and secure is one of the most significant business decisions that an organization will ever make.

You just can't afford to go wrong...

However, just when you think you've considered everything and done it all, something happens, and you lose the data you have been storing over the years. How do you continue making critical business decisions? How are employees able to perform daily tasks? All your data is now gone or stolen!

# Where Did You Go Wrong?

Having established a successful business, you failed to take precautions to keep your data safe and protected from situations like malfunctioning storage devices, failure of an operating system, accidental damages, or deletion of files. Most of all you did not prepare well for data loss due to *human error.* There are a couple different types of damage that can occur:

- **Physical Damage:**
  Human error or natural disasters could be the prime reasons for physical damage to your data. Mechanical failures of the hard disks, PCB failures, or failed motors, any of these can happen without warning, and your data can just vanish.

- **Logical Damage:**
  Damage to data can also result from corrupt file systems and partitions, media errors, overwritten data, lost or reformatted data, deleted data, and bad sectors.

# Early Steps to Protect Your Data

You must start somewhere, but it doesn't mean that you stop. Protecting data is a continuous process. As your business evolves, your data protection and recovery plans should evolve as well. Identifying critical data and conducting a risk analysis are the first steps in data recovery, but these will need to be evaluated regularly.

## STEP 1:

### Identify Critical Data

When you start to think about the amount of data that moves back and forth on your company network each day, you begin to realize how important it is to keep it safe. It would be impossible to remember and recreate every email, every customer order, every spreadsheet, and document. Therefore, when developing a data recovery plan, it's essential to understand what data is critical for restoring fundamental business processes and operations.

The best way to do this is to take the following steps:

- **Map the data.** Ask yourself: Where does data belong? How is the data managed?

- **Identify responsibilities and obligations**. Ask yourself: What are your responsibilities for protecting data concerning agreements, NDAs, internal policies, and other important documents?

## STEP 2:

### Conduct a Risk Analysis

A risk analysis will help you identify and define threats that will compromise your data. It needs to consider internal and external factors that can be analyzed to see how each one will affect the company.

Evaluate current measures in place for data protection to discover gaps that will compromise your data. A risk analysis should include the following steps:

- Identify the risks
- Scope the analysis
- Collect data about the risks
- Document the threats identified
- Define what processes are already in place
- Prioritize the risks

## STEP 3:

### Break It Down

A successful data recovery plan requires having detailed plans and procedures that support the overall security goal. Build a team to implement the policies and verify that they are executed correctly.

An essential item and one not to be overlooked is the **Data Backup Plan**. The backup plan is necessary for every data recovery plan because it must be backed up correctly to recover lost data. The data backup plan should include the following:

- What is included in the backup?
- What technologies and storage resources are used?
- How do you handle unsuccessful backups?
- What are the detailed backup testing procedures?
- How often will the plan be evaluated and updated?

Once you create procedures and any additional plans, build a checklist to ensure that all steps are defined, assigned, and followed, so there's accountability.

## STEP 4:

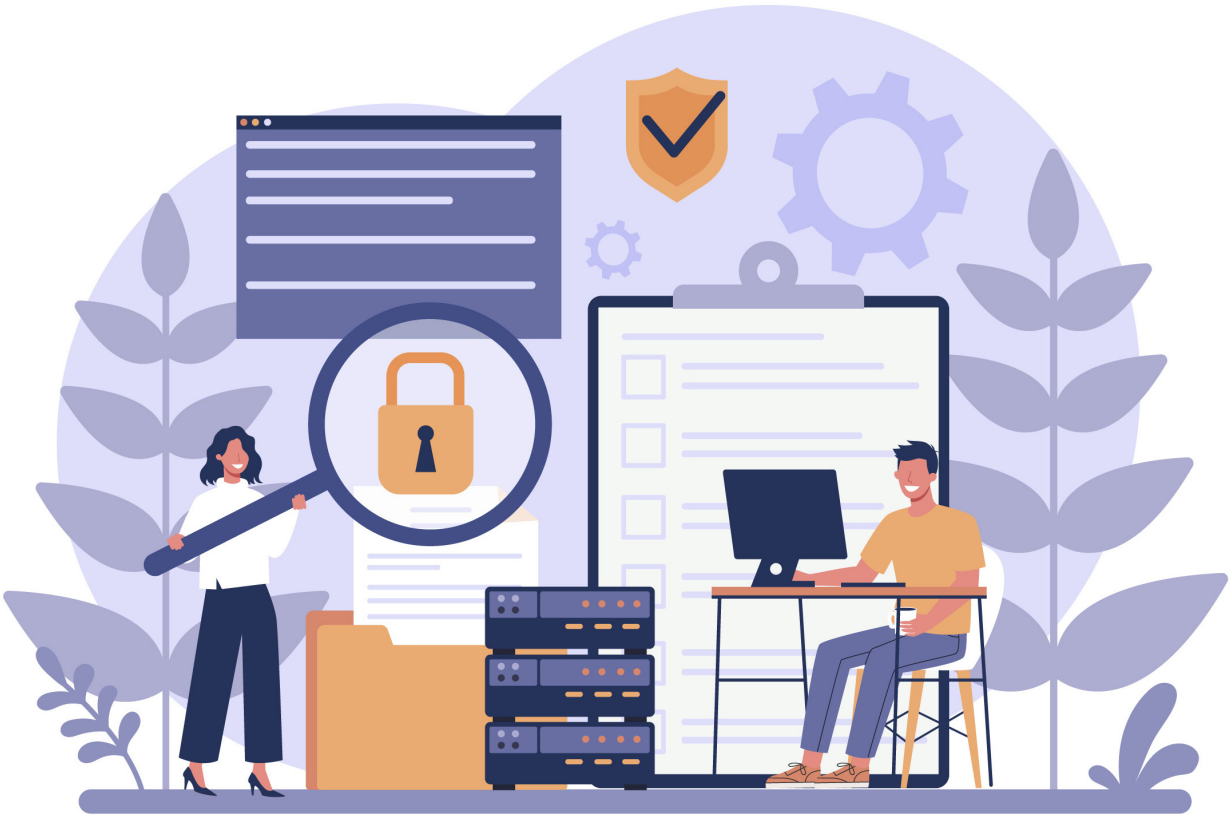
### Test, Test, Test and Test Again

Once you've built your data recovery plan, you're ready to test it. There are multiple ways to test your plan, but following best practices will help provide optimal testing and give you the best results. Anytime you conduct a test, you should review the other areas of the plan to determine if other updates or changes are needed.

# Testing Best Practices

When testing effectively there are a few key pointers you'll want to keep in mind:

- **Conduct regular and thorough tests.** Testing the plan regularly will ensure that there will be only a minimal interruption to business systems if there is ever a data loss.
- **Set measurable benchmarks.** RTO (recovery time objective) and RPO (recovery point objective) are measurable identifiers that explain the method, frequency, and even the location of all backups which you'll need to make sure you're on track.
- **Keep team members active.** Assign team members a specific area of the plan that they're responsible for, such as researching, developing, updating, implementing, and testing.



# Types of Tests

There are several different types of tests which gauge different key aspects.

- **Paper test.** Teams and individuals read and annotate data recovery plan documents
- **Walk-through test/tabletop test.** Review the plan with senior leadership to identify any issues or necessary modifications. It can also involve management and team members reviewing scenarios and discussing what actions should be taken.
- **Simulation test.** A run-through to practice a simulated data loss and gauge the effectiveness of the emergency response plan.
- **Parallel test.** Involves setting up a duplicate system that mirrors the real one, performing actions on both, and seeing if the outcomes are similar.
- **Cutover test.** Similar to a parallel test, but on this test, primary systems are completely shut down to see if the recovery system can handle a full workload.
- **Full-scale test.** A comprehensive test that provides a realistic experience to expose any flaws and critical areas needing to be addressed. This is the best test for thoroughly testing for any areas of weakness and obtaining the most information.

# Testing Frequency

It's critical to test on a regular basis; otherwise, you're putting the company at a significantly higher risk of failure when there's a system breach or disaster hits. There are different factors to consider when determining how often to test, including company size and the amount of critical data you need to protect.

It seems that the standard frequency for backup recovery tests is yearly. However, as the number of security breaches increases and your chances of being attacked keep rising, you should test your plan quarterly. You can work with your MSP to determine how often you should test based on the factors above.

# Putting It Altogether

Large enterprise organizations may manage building, testing, and implementing a data recovery plan, but small businesses won't have the resources to do that. Small businesses can lean on the expertise and experience of a backup and recovery service provider such as Visual Edge IT™. Partnering with a backup and recovery service provider will give business owners confidence that their data is protected and recoverable if lost or stolen.

VISUAL EDGE IT™

SECURE TECHNOLOGY SOLUTIONS

6050 Corporate Way
Indianapolis, IN 46278
**(866) 863-2266**

**learnmore@visualedgeit.com**
**www.visualedgeit.com**
**@visualedgeit**