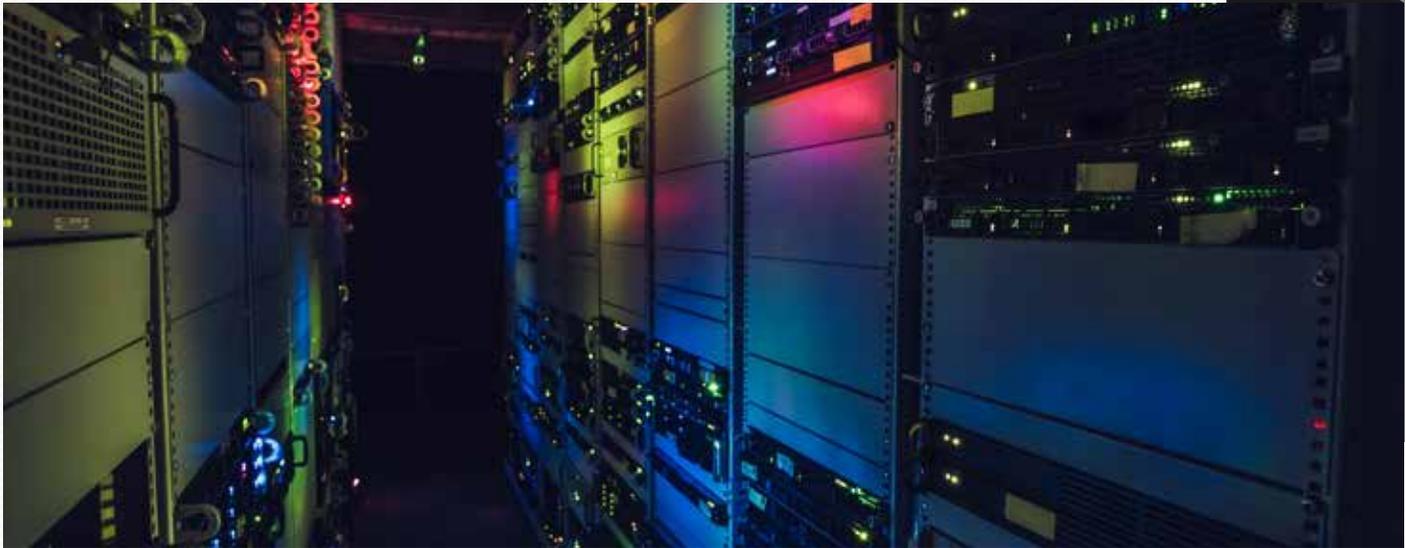
A man in a white shirt and tie is pointing at a server rack in a data center. He is holding a tablet that displays a complex data visualization with various colored bars and lines. The server rack has several units with glowing lights and cables.

VISUAL EDGE IT

YOUR BDR PLAN IS MORE
THAN JUST YOUR BACKUP
(IT'S YOUR LIFELINE)

BDR stands for **backup** and **disaster recovery**. As the name implies, it's a plan crafted by businesses to recover their operations in the event of a catastrophic disaster.

Not all disasters are created equal. Most people tend to equate disasters with tidal waves, hurricanes, furious fires, and earthquakes – basically, all kinds of natural disasters. However, there are many more likely threats that can bring your organization to its knees.



RANSOMWARE

Viruses and malware (specifically ransomware) have proven time and time again to be extremely dangerous. Ransomware attacks caused 22% of infected small- and medium-sized organizations to cease business operations immediately.

Once ransomware takes hold of your files and folders, it will systematically lock and encrypt each individual piece of data.

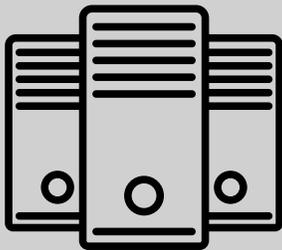
There are only two ways to recover your information. You can pay the data ransom, possibly costing thousands of dollars and offering no guarantee of data retrieval. Or, you can [recover most if not all of your files quickly from a data backup](#).

INSIDER THREATS

People make mistakes all the time. Sometimes, these mistakes are as simple as deleting a single file. Other times, people may delete entire back-end databases, causing hosted applications and services to crash indiscriminately.

Sometimes, the damage isn't accidental at all. Privileged users, such as managers with access to sensitive information, pose the [biggest insider threat](#) to organizations (60%). This is followed by contractors and consultants (57%), and closely by regular employees (51%).

To mitigate both accidental and purposeful damage done to systems, many companies turn to data backups. As long as these backups are secure, organizations can restore lost data without a hitch and continue operations as normal.



“IT’S NOT ALWAYS THE ENTIRE MACHINE THAT FAILS. IN THE USA, APPROXIMATELY **140,000 HARD DRIVES** FAIL EVERY WEEK.”

OUTDATED HARDWARE

It's hardly a disaster in the traditional sense, but having old hardware fail in the midst of daily operations can be devastating. If an old server decides suddenly to breathe its last digital breath during the workday, you'll be stricken with downtime.

It's not always the entire machine that fails. In the USA, approximately [140,000 hard drives](#) fail every week. These hard drives often contain business-critical files that throw a wrench into business operations.

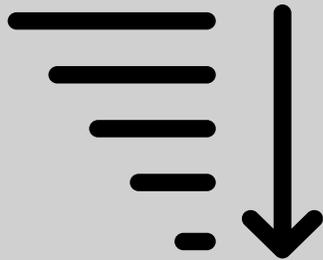
Having consistently backed up data gives companies a restore option once they replace the failed hardware.

HOW BDR PLANS FIT INTO IT ALL

Each example listed is a very real disaster to businesses. The answer to most of the problems is clear – back up your data to save the day. That's the “B” in BDR.

The “DR” part comes between the initial downtime and the full recovery. Without a disaster recovery plan in place, organizations have a very difficult time coordinating recovery efforts and defeating downtime.

ITIC's latest survey data finds that [98% of organizations](#) say a single hour of downtime costs more than \$100,000. In the end, the entire point of disaster recovery efforts is to avoid downtime.



“ITIC'S LATEST SURVEY DATA FINDS THAT **98% OF ORGANIZATIONS** SAY A SINGLE HOUR OF DOWNTIME COSTS MORE THAN **\$100,000**.”

Disaster recovery plans should cover several key points. These include:

- Who should be in charge during recovery, and what their roles consist of
- Contact information for all mission-critical employees, including phone numbers and email addresses
- Prioritization of the most business-critical systems for recovery organization
- Clear definitions of when and where to rendezvous at an alternative worksite

While general, this list of priorities gives a good general view of the necessary components of a disaster recovery plan. The most important aspect of all is to constantly test the plan and backups to ensure full functionality.

After all, the plan and backups are useless to you if they don't work when you need them most.

BDR PLANS ARE YOUR LIFELINE

We've said it before, and we'll say it again – the BDR plan is the lifeline of your business. When disasters occur, you'll surely suffer from downtime. But when you have a BDR plan ready to go, you can survive this threat with minimal consequence.

In fact, you can use these plans to completely dodge the nasty financial, reputational, and operational damages caused by downtime.

Interested in [learning more about BDR plans](#)? Want to know some tips from industry experts on how to beat downtime? [Contact us](#) and we can work together to save your business from any disaster that comes your way.



Toll Free: (866) 863-2266 | Service Desk: (317) 275-3770

VisualEdgeIT.com