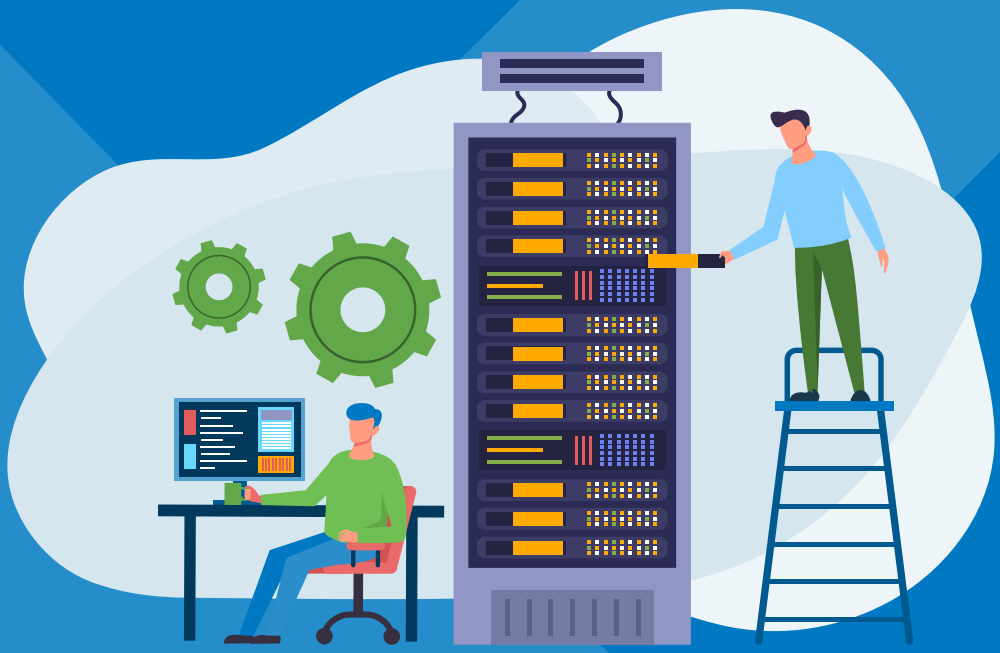
A Comprehensive Guide to

Data Backup & Disaster Recovery

FROM THE MANAGED SERVICES EXPERTS AT TPX



Executive Summary

Businesses are under the growing threat of financially devastating cyberattacks, with successful data breaches resulting in significant data loss and leaving companies at the mercy of repeat ransomware attacks.

This Comprehensive Guide to Data Backup & Disaster Recovery discusses the following:

- What is backup and disaster recovery?
- What are backup and disaster recovery solutions and deployment options?
- Why should businesses invest in backup and disaster recovery solutions?
- What should businesses look for in the right backup and disaster recovery solution?
- Should businesses insource or outsource their backup and disaster recovery solution?
- What should businesses look for in an MSP?
- Why should businesses choose TPx for endpoint management and security?

This guide details everything you need to keep your data backed up and recoverable in the event of a cyberattack.

Key Takeaways

Both backup and disaster recovery solutions should be deployed for a complete BDR solution.

More than half of businesses don't have enough budget to recover from data incidents.

75% of small businesses don't have a disaster recovery plan.

Organizations should employ the 3-2-1 Rule for backup and disaster recovery.

Table of Contents

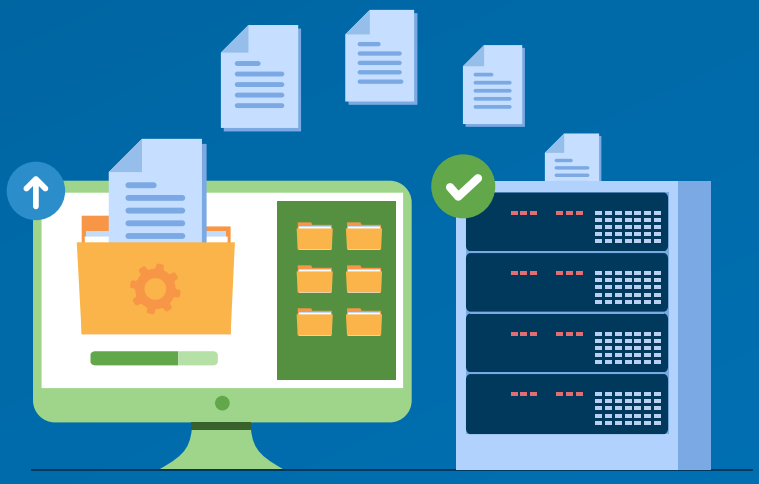
PART 1

What is Backup & Disaster Recovery?

What is Backup?

Backup refers to the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure, security breach or catastrophe. The process of backing up data is pivotal to a successful disaster recovery plan.

Enterprises back up data they deem to be vulnerable in the event of buggy software, data corruption, hardware failure, malicious hacking, user error or other unforeseen events. Backups capture and synchronize a point-in-time snapshot that is then used to return data to its previous state.



Backups can take many forms, such as:

- **Duplicating data** on secondary storage arrays in your primary data center
- **Backing up data** to a remote data center
- **Offloading data** to a public cloud or multiple clouds for extra protection

What is Disaster Recovery?

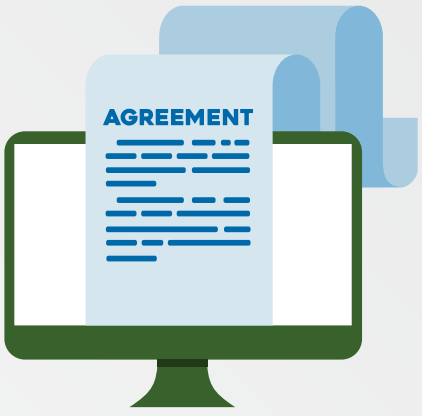
Disaster recovery (DR) is an organization's ability to respond to and recover from an event that negatively affects business operations. The goal of disaster recovery solutions is to enable the organization to regain use of critical systems and IT infrastructure as soon as possible after a disaster occurs and to minimize any data loss associated with the disaster. To prepare for this, organizations often perform an in-depth analysis of their systems and create a formal document to follow in times of crisis. This document is known as a disaster recovery plan.

Why Do You Need Both?

Backup is a part of disaster recovery, but it's only one component. Disaster recovery encompasses a complete process for safeguarding data and restoring them. In certain situations like storing files that aren't mission-critical, backup may be all you need to protect certain parts of your infrastructure or business against disruption. But it's not a total solution.

Disaster recovery is vital for protecting services and network infrastructure (servers and central databases) that your business depends on to operate on a daily, if not hourly, basis. A DR solution ensures you can restore data and services in real-time before your business operations stop in its tracks.

Additionally, there are consequences to consider beyond your internal operations. Depending on your business model, you may have service level agreements (SLAs) to which you're contractually obligated to adhere to and deviation from may result in severe financial and legal repercussions. Being inoperable for an extended period of time legally may not be an option for your company. Data backup alone may not fully address this need.



PART 2

Why Invest in Backup & Disaster Recovery Solutions?

Now that you understand what BDR solutions are and the different deployment models, the question is, why make the investment in these solutions in the first place?

Backups are important because they provide a way to recover your data and systems in the event of data loss or data corruption. There are many potential causes of data loss, including hardware failures, software bugs, human error and cyberattacks. Without backups, you may be unable to access or recover your data, which can be costly and disruptive to your business.

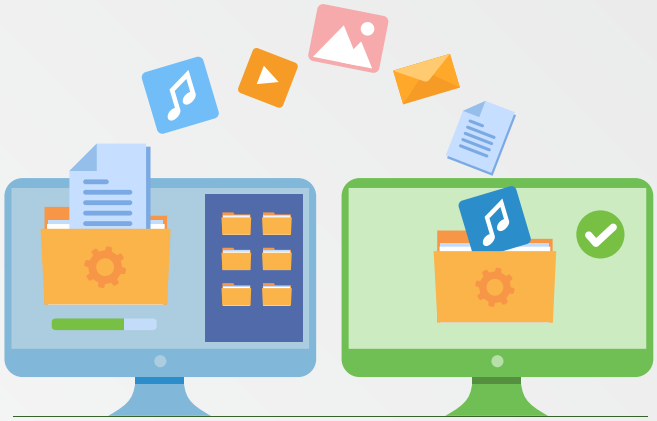
In addition to helping you recover from data loss, backups can also be useful for:

- **Upgrading or replacing hardware or software —** Backups can help you migrate your data to a new system without losing any important information.
- **Disaster recovery —** In the event of a natural disaster or other catastrophic event, backups can help you restore your systems and data quickly and efficiently.
- **Compliance —** In certain industries, such as healthcare and finance, it may be required to maintain backups to meet regulatory compliance requirements.

Overall, having regular and reliable backups is an important part of any data protection strategy. In the event of data loss, backups can save you time, money and frustration and help ensure that your business can continue to operate smoothly.

Many businesses think “It won’t happen to me.” Think again:

- 43% of cybersecurity attacks happen to SMBs (Microsoft)
- 50% of SMBs experienced a data breach (Ponemon Institute)
- 33% of business downtime is caused by IT equipment failures (Singlehop)
- 67% of small businesses have experienced data loss due to various causes such as hardware failure, human error and cyberattacks, according to a survey conducted by Carbonite, a cloud backup provider. The same survey found that 52% of small businesses do not have a formal data backup plan in place.
- $133,000 is the average cost in lost revenue and recovery for small businesses hit by ransomware attacks, according to a study by the Institute for Critical Infrastructure Technology.
- 35% of consumers regularly back up their data, while 43% have never backed up their data, according to a survey by IDrive, a cloud backup provider. The same survey found that 38% of respondents lost important data due to a hardware failure, and 27% lost data due to a software malfunction or human error.



What Challenges Do Backup & Disaster Recovery Solutions Solve?

BDR solutions primarily protect a company from the financially and reputationally disastrous effects of a successful data breach.

Data Disaster Risks by the Numbers

140,000 hard drive crashes happen weekly in the U.S.

Every five years, **20%** of small and medium-sized businesses suffer from data loss due to a major disaster.

60% of businesses suffering a data loss incident will shut down within six months.

93% of entities losing their data center for 10+ days file for bankruptcy within one year of the incident.

96% of businesses don't back up their workstations.

MORE THAN HALF of businesses don't have enough budget to recover from data incidents.

93% of organizations that suffer a major data disaster and don't have a recovery plan will go out of business within one year.

3 of 4 of small businesses lack a disaster recovery plan.

Source: https://webtribunal.net/blog/backup-statistics/#gref

What Are Real-World Success Stories for Backup & Disaster Recovery Solutions?

Construction Firm Virtualizes Failed Server

TPx was engaged by a home builder in the Dallas area to manage its existing servers and workstations, deliver an improved Backup & Disaster Recovery solution, and upgrade/replace the main server, which was several years old and becoming increasingly unstable.

Phase 1 of our solution included implementing Managed Endpoints and Managed Backups to ensure that we could effectively manage the server and deploying a solid backup and DR solution to protect it.

Before we moved to Phase 2 in which we planned to replace the old server, it experienced a major failure. Using the Managed Backup “Instant Virtualization” feature, this customer could run the failed server as a Virtual Machine on a backup appliance and keep their business running until the new server could be installed.

Municipality Restores Tax Data With Backup Service

A municipality in Maine engaged TPx to deliver a Backup & Disaster Recovery solution that would better meet its recovery time objective (RTO) and recovery point objective (RPO). TPx deployed Managed Backup Optimum for this customer to protect its critical systems and data. TPx and our solution were put to the test when the tax collector mistakenly uploaded the incorrect data into the tax application and, at the same time, erased the last backup from the system. TPx was called to help recover from this catastrophe.

Within minutes, TPx was able to resolve the issue by recovering the data from a backup copy stored on the local Managed Backup device. This backup copy restored all the correct data from 15 minutes prior to the event and the tax collector could then finish working and get all the tax bills out to the community on time.

Real Estate Firm Restores Accounting Data

A small commercial real estate management firm in Maine uses TPx managed IT services. Our customer called in a panic as she had accidentally deleted the company's QuickBooks data off the shared drive. This was all the company's accounting data and if lost, would have put the company at significant risk. Luckily, the company uses our Managed Backup solution. TPx technicians located the last clean backup of the QuickBooks data and quickly restored it, preventing a catastrophe that could have resulted in a significant financial impact on the organization.

Restaurant Recovers Failed Exchange Server

A west coast restaurant chain engaged with TPx to provide a new Backup & Disaster Recovery solution that would better protect their existing IT environment. At the same time, they were preparing to migrate from an on-premises Exchange email server to Microsoft Office 365 to enhance their communications experience and reliability. Shortly after the implementation of our Managed Backup service, the customer experienced a major failure of their in-house Microsoft Exchange server. Because this server was backed up every 15 minutes by the Managed Backup on-site backup appliance, TPx could recover the failed server from a recent backup image and run it as a Virtual Machine on the backup appliance. This allowed the customer not only to keep email communications up and running, but also to complete the migration to Office 365 using the temporary server, saving significant downtime and the cost of replacing a failed server just to migrate off it weeks later.

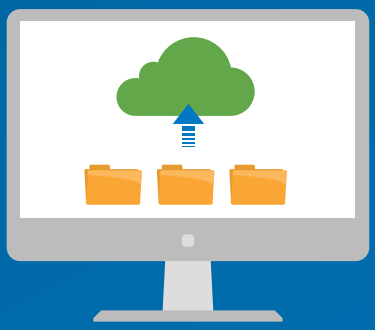
PART 3

What Are Backup & Disaster Recovery Solutions?

Now that you have an understanding of backup and disastery recovery, let's look at the solutions that you can deploy to protect your organization.

What Are the Types of Backup & Disaster Recovery Solutions?

The major types of backup and disaster recovery solutions include full backups, incremental backups and differential backups:



- **Full Backup —** A full backup is the starting point for all other backups and contains all the data in the folders and files selected to be backed up. Restoration from a full backup is quick, but backing up all data each time is extremely slow and in almost all cases is not feasible.
- **Incremental Backup —** Incremental backup stores all files that have changed since the last full, differential or incremental backup. The advantage of an incremental backup is that it takes the least time to complete. However, during restoration, each incremental backup must be processed, which lengthens recovery time.
- **Differential Backup —** The differential backup contains all files that have changed since the last full backup. Differential backups shorten restore time compared to incremental backups. However, performing a differential backup too often can grow it beyond a full backup.

Backup-as-a-Service (BaaS) Versus Disaster Recovery-as-a-Service (DRaaS)

BaaS and DRaaS can be viewed as simply outsourcing management, monitoring and maintenance of backup and disaster recovery to a third-party managed services provider (MSP). However, BaaS and DRaaS differ significantly in terms of the capabilities and responsibilities required by the MSP to implement them. Below is a basic breakdown of the differences between BaaS and DRaaS.

	BaaS	DRaaS
Scope	BaaS only backs up data.	DRaaS backs up data and infrastructure.
Recovery Timeline	BaaS can perform data recovery, but RPO and RTO are usually measured in hours or days.	DRaaS RPO and RTO are usually measured in seconds or minutes.
Costs	BaaS costs are lower than DRaaS costs.	DRaaS costs are higher than BaaS costs.
Resource Consumption	BaaS is a storage-based service with fewer allocated resources than DRaaS.	Additional resources are involved in DRaaS, including replication software, compute and networking infrastructure.
MSP Responsibility	With BaaS, the MSP is responsible for maintaining and managing backups.	With DRaaS, the MSP is responsible for the failover process from the affected primary environment to the replicated remote environment. The provider also monitors disaster recovery operations, helps customers recover systems and assists in the return to normal daily business operations.

File-Based Versus Image-Based Backup

What is File-Based Backup?

With file-based backup, only specific files or folders are backed up. The “System State” (operating systems, logs and applications), is not backed up. As such, to recover a failed system fully using a file-based backup system, a skilled IT administrator would need to re-install and configure the operating system, install and configure the applications, “mount” the backup and then restore the data. Data restores are done on a “one file at a time” basis. This is a slow process that is prone to failure due to all the manual steps involved.

What is Image-Based Backup?

An image-based backup copies an image of the entire machine. This image contains the “System State” and all data. Backing up the full image allows for faster and more flexible restores of protected devices with less manual intervention and resources required when compared to a file-based backup solution. It also allows the restoration of dissimilar hardware or virtual machines.

What’s the Difference Between File-Based & Image-Based Backup?

File-based backup can back up single files or a selection of multiple files, whereas image-based backup will create a backup copy of your whole system or selected partitions. An image-based backup is much larger compared to a file-level backup and can take multiple hours to backup.

When to Use

File-Based Backup

Use file-based backup when you need to recover single files or folders in case of accidental data deletion.

Image-Based Backup

Use an image-based backup to recover your entire system, including partition settings, installed solutions and data.

What Are Backup & Disaster Recovery Deployment Options?

Businesses have a few options to choose from when deploying their backup and disaster recovery solution, including local backup, cloud backup and hybrid local and cloud backup.

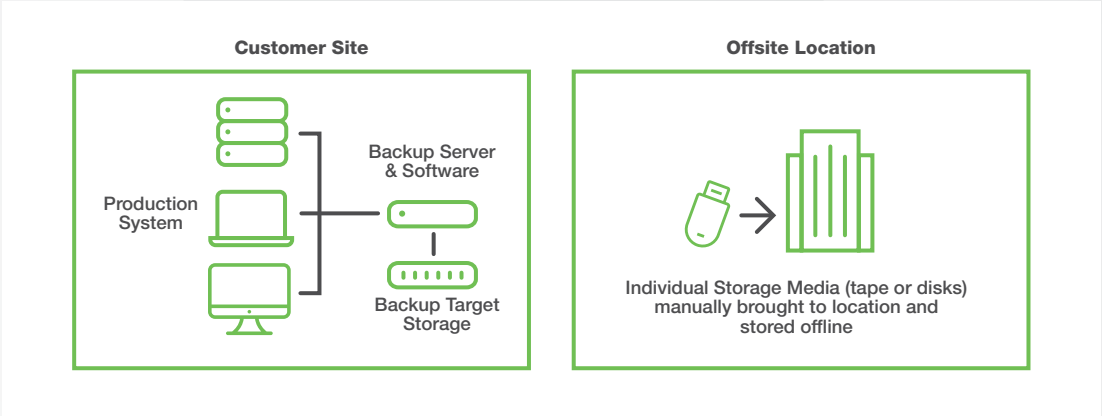
Local Backup

A local backup is an on-premises backup of your systems, applications and data to a local device, such as tape, disk, hard disk, flash drive, CD, external hard drive or other media that is located on-site near the source of the data. A more effective local backup strategy requires a second backup on a different device stored off-site to ensure data protection.

Server & Storage

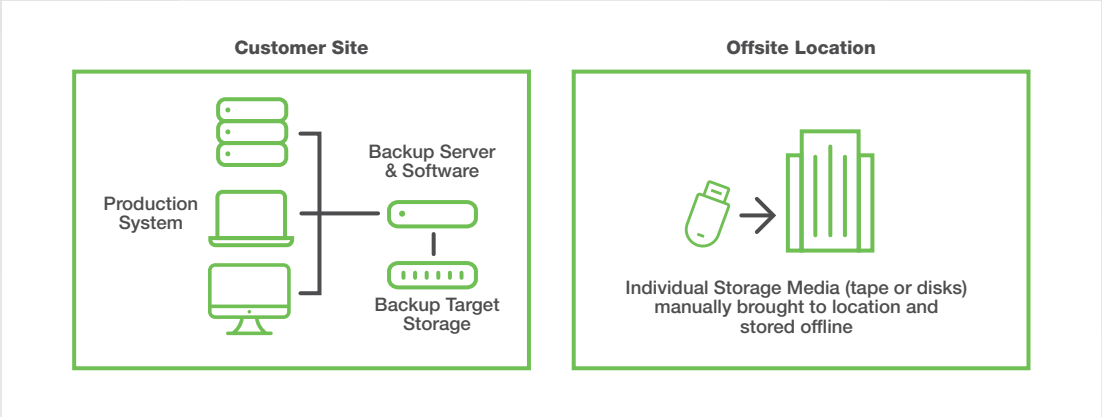
A traditional local backup solution uses a “Target" server with backup software on it to manage backups. Production servers also typically have a backup software agent installed. The backup target server manages backup jobs, sending data to local storage (disk or tape). There is no offsite data transfer other than the system administrator physically taking backup media offsite. These are often file-based backups that require additional resources and time to recover from a system failure.

This solution type also typically limits the backup interval (how many times per day you back up), which creates an increased risk of data loss. There’s no option for local instant virtualization, so when a protected server fails, it’s down and users are unable to work until it’s repaired.



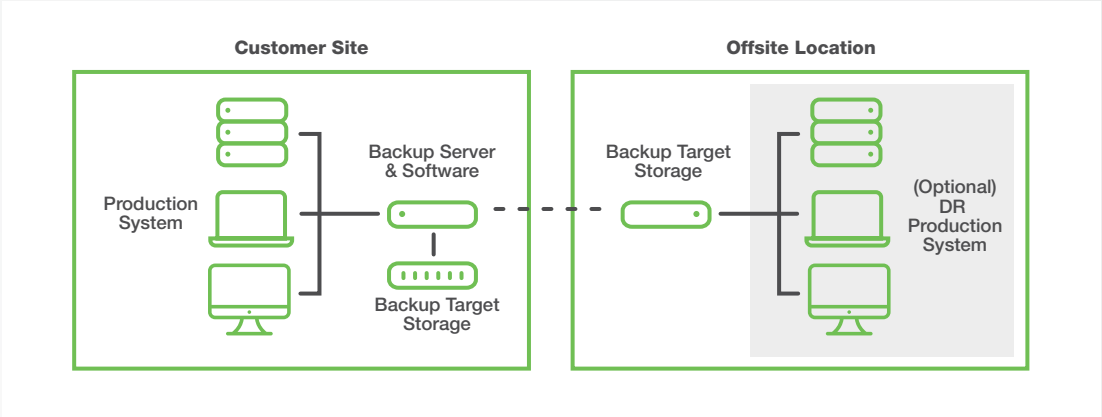
Appliance

This solution uses a purpose-built backup appliance that combines the functions of the backup target server, local storage target and backup software. This type of solution typically delivers faster and more efficient local backups than the traditional server and storage solutions but without offsite protection, they still have many of the same challenges. Solutions often have options for cloud replication but a business may choose not to use the offsite cloud replication to “save money.” Some solutions will have the ability to do instant virtualization and some will not.



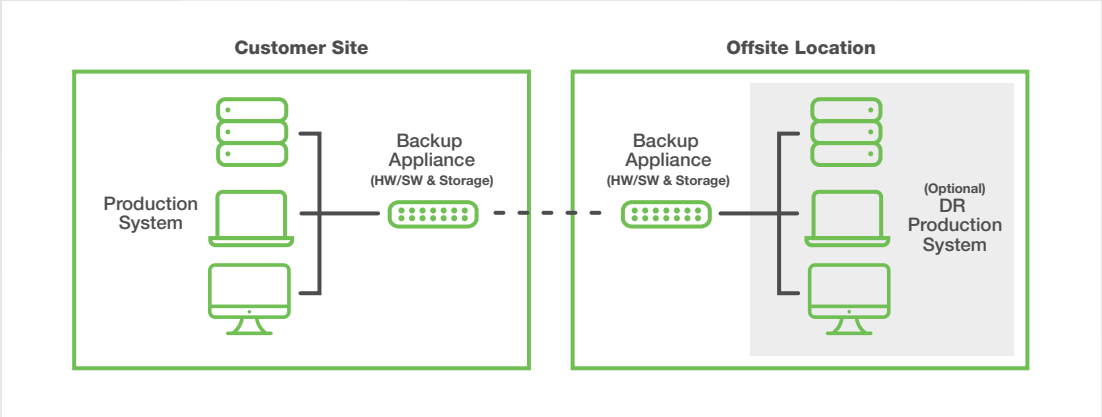
Replication to Second Site – Servers & Storage

This solution has the same challenges as "Local Backup – Server & Storage" except the customer is replicating data to a second offsite location so data is automatically protected offsite, such as a colocation facility or a secondary customer site. With this deployment model, businesses benefit from having offsite replication but face additional costs for colocation and storage infrastructure at that location. Optionally, additional production server infrastructure may be at the location as well. Without it, the offsite location only serves as a place to safeguard backups; with it, the offsite location can be a production facility in the event of a primary site failure. All of this creates additional management and administration cost. Even if the customer uses their own data center or office facility as the secondary site, they still incur the costs of space, power, equipment, bandwidth and management, at this location.



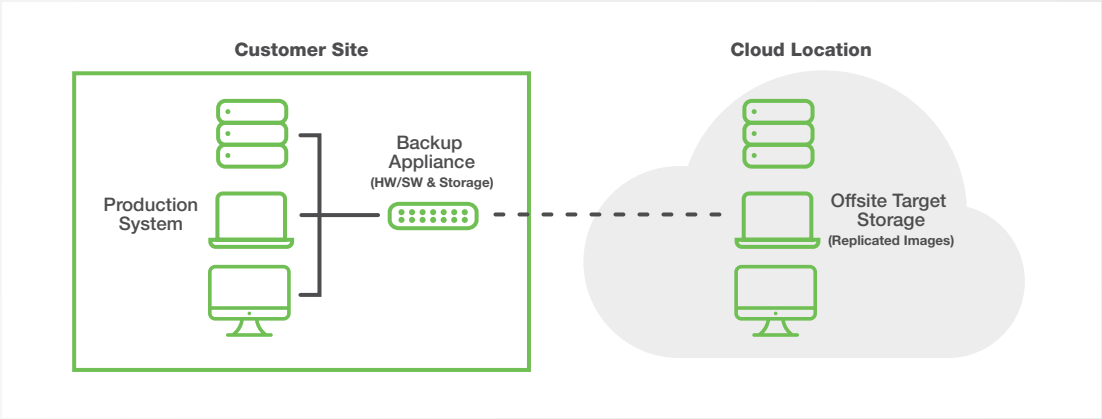
Replication to Second Site – Appliance

This solution has the same challenges as "Local Backup - Appliance," except the customer is replicating data to a second offsite location. With this deployment model the client benefits from having offsite replication but faces the additional costs of the colo facility and the second appliance at that location. This also creates additional management and administration costs. The customer could use their own data center or office facility as the secondary site, but they will still incur the costs of space, power, equipment, bandwidth and management at this location.



Cloud Backup

Cloud backup will backup an organization's systems, applications and data to a cloud-based server in a remote location. This server can either be private or public. Some larger enterprises have the resources and budget to maintain a private cloud infrastructure, while smaller organizations typically use a public cloud service, which supports multiple tenants. With a public cloud backup service, the infrastructure is managed by the provider and organizations pay a subscription to use the service.

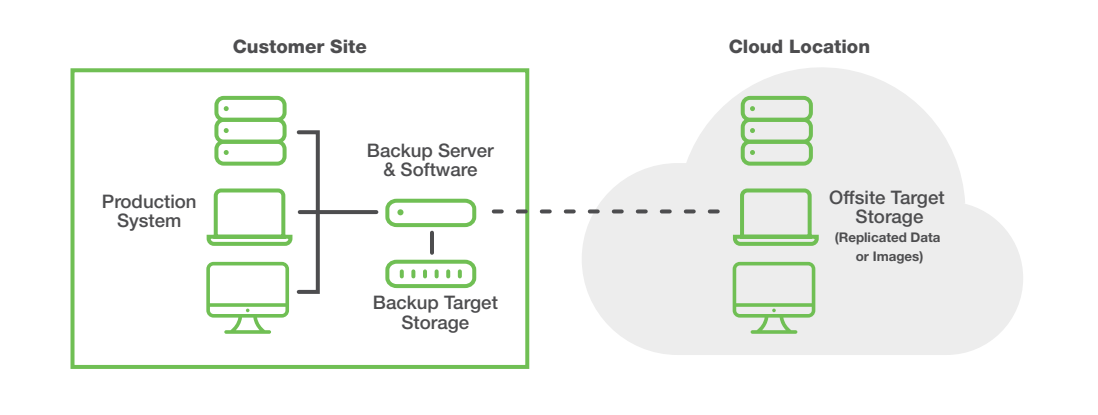


Hybrid Local & Cloud Backup

A hybrid backup solution involves both local backups and a cloud-based backup. Remote cloud servers are linked and synced with local backup resources to offer off-premises recovery points in the event of a disaster. The cloud backup functions as the backup to the local backups.

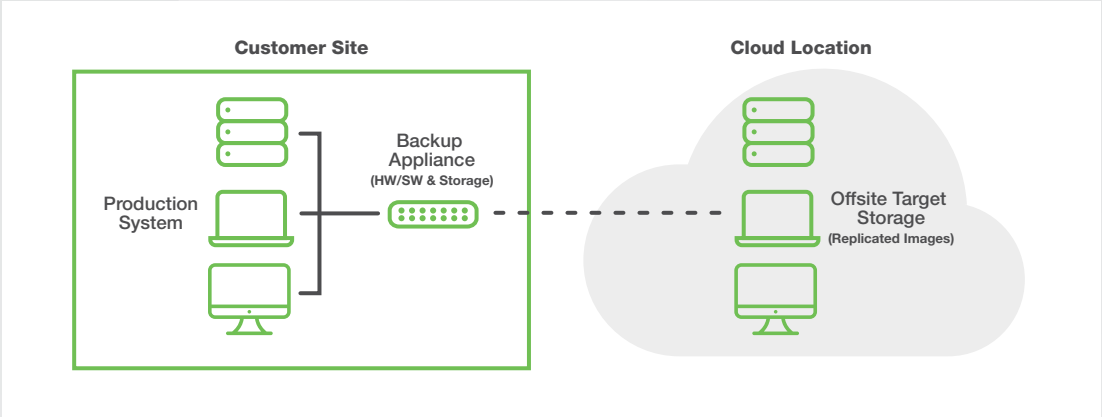
Hybrid Local & Cloud Backup - Server & Storage

This solution includes a local disk-based backup as explained in "Local Backup – Server & Storage" but then uses replication software to push data into a public cloud. Typically, the client will have software that backs up locally and then replicates to the cloud. The client pays for the storage and infrastructure in the cloud -- costs that can grow over time. For example, a 1TB full backup with 10 years of incremental data is larger and more expensive than the initial 1TB backup. Some private cloud pricing models cost more as storage needs grow. Depending on the provider, they may or may not have the ability to virtualize and run protected servers in the cloud. Also, often the local server/storage used is the same as the production environment, which increases risk; if the production hardware is down, backups are not accessible.



Hybrid Local & Cloud Backup – Appliance

TPx's Managed Backup solution uses the hybrid local and cloud deployment model. It includes a purpose-built backup appliance that includes all hardware and software to conduct local backups and automatic replication to a private cloud. Many vendors are developing hybrid solutions and this deployment model is predicted to account for nearly two-thirds of the backup and disaster recovery market over the next 10 years. Instant virtualization provides significantly lower RTO than solutions that do not have this feature and therefore reduces the duration and cost of downtime significantly.



PART 4

How Can Businesses Choose the Right Backup & Disaster Recovery Solution?

Backup and disaster recovery is a complex solution that fits into your organization's overall business continuity plans, making the decision to select a high-quality solution a critical one.

What Are Key Considerations in Backup & Disaster Recovery Planning?

There are several key considerations to keep in mind when creating backups of your data:

- **Frequency —** It's important to create backups on a regular basis. The frequency of your backups will depend on how quickly your data changes and how much you can afford to lose.
- **Storage location —** Your backups should be stored in a secure location that is separate from your primary data. This could be an external hard drive, a cloud storage service or a physical offsite location.
- **Encryption —** Consider encrypting your backups to protect them from unauthorized access.
- **Testing —** It's important to test your backups to ensure that they're successful and that you can restore your data in the event of a data loss.

- **Versioning —** Keep multiple versions of your backups so that you can go back to a previous version if necessary.
- **Automation —** Consider automating your backup process to ensure that it is done consistently and on schedule.
- **Documentation —** Keep detailed documentation of your backup process, including the frequency of backups, the location of backups and the process for restoring data from backups. This will be helpful in the event that you need to restore your data from a backup.

Businesses should address the following components as part of their backup and disaster recovery planning:

Downtime

How much time can you afford to be down before it causes an impact on your business? What is your recovery time objective?

Data Loss

How much data can you afford to lose before it causes an impact to your business? What is your recovery point objective?

What Solutions Best Match Your Recovery Point Objectives & Recovery Time Objectives?

RPO (Recovery Point Objective) and RTO (Recovery Time Objective) are measurements that quantify the level of disruption your business can tolerate before critical damage occurs.

What is RPO?

RPO is the maximum amount of data that can go out of sync, measured by time, following a disaster that is acceptable to the organization.

What is RPO?

RTO is the amount of time in which a service or data must be recovered following an outage in order to avoid negative operational, financial or legal outcomes for your business.

Different solutions are better suited to certain RTOs and RPOs, so it's important to work with a qualified expert to help you decide what might work best for your company.

What Are Common Mistakes Businesses Make with Backup & Disaster Recovery Planning?

When selecting a backup and disaster recovery solution, businesses tend to make these mistakes:

MISTAKE 1
Not understanding your business objectives.

Performing a Business Impact Analysis (BIA) can help you understand your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) so you can invest in the right BDR solution. Confused? Let's translate this tech lingo into "plain English."

The first step in evaluating any BDR solution is to understand the impact that system failures or data loss can have on your business. Ask yourself these three questions:

What data do I need to protect?
Do you have mission-critical data such as customer records, inventory or accounting information? Identify where this data is stored and which systems run the apps that use it.

How much data can I afford to lose in the event of a failure?
This is your RPO. If you lost your sales transaction records, shipping data or case files that were created or updated over the last hour, how would that impact your business? What if you lost that data for a whole day or even a week?

How long can I afford to be down in the event of a failure?
This is your RTO. If you couldn't process sales transactions, access inventory or get that important RFP delivered on time, how much would your business suffer? Would you lose revenue? Customers? Reputation?

Ask yourself these three questions, and use the answers to establish your goals (for example, "I need this system back up and running in four hours" or "I can't lose more than two hours of this data"). Then you should be able to understand whether your existing BDR solution allows you to meet these goals. Don't guess – know – how much time and how many resources it would take to restore a file, a database and a complete server.

MISTAKE 2

Focusing on the backup, not the recovery.

It's called backup and disaster recovery for a reason. Yes, your data is important and you need to have it backed up. However, the real value is when the data is available to you so that you can run your business.

That means you need to be able to quickly and efficiently restore failed systems and lost data to truly meet the business goals you've established in your Business Impact Analysis. With many traditional onsite or cloud-only backup solutions, restore time may take many hours or even days. Make sure your solution isn't one of them.

Consider this example:

Your main application server experiences a hardware failure and crashes. You contact the manufacturer, who will be there the next business day with the parts to get the server back up and running. Let's presume the work is completed by midday the day after the failure. Now you must restore the operating system, the application files and all the data on to that server before you can conduct business again. This process will take several hours to complete.

At this point, you've been down for at least two days. Does that meet the business goals you established earlier? Today's backup solutions offer advanced technology and capabilities that can get you back to business within minutes or hours, instead of days -- all of which can translate to thousands of dollars in savings.

MISTAKE 3

Not protecting data offsite.

Protecting your data onsite is a must, right? This makes for faster and more efficient restores of files, folders and even complete systems. But what would happen if your entire site were impacted by a fire, flood or other disaster? If your production systems and your backup data are in the same location, you could lose everything.

Modern BDR solutions deliver automatic and secure replication of data, and in some cases complete system images, to the cloud. This ensures that your data and systems are available when you're ready to get back to work.

MISTAKE 4

Not actively managing your backup.

Merely deploying a great BDR solution doesn't ensure that your business is protected over time. Backup jobs fail. Data, systems and applications change. An effective BDR solution requires focused attention from skilled resources to configure backup jobs as needs change, monitor backup job success, resolve failures and maintain the technology. This is a challenge for all businesses, but especially SMBs, who typically have limited IT resources.

If these important functions are not addressed consistently, it can lead to failed or corrupted backups, missing backups or other issues that can prevent you from restoring the data you need. To solve this challenge, many SMBs are looking to outsource Backup and Disaster Recovery to a managed service provider like TPx.

MISTAKE 5

Not testing restores.

As mentioned earlier, the majority of SMBs are not prepared for data loss, but they only figure this out after a disaster hits and they can't successfully restore their data. You can alleviate this concern by testing your backups ahead of time to ensure they're recoverable.

Unfortunately, fully testing backups can be a complex and expensive endeavor, which is why SMBs very rarely perform regular testing.

Today's leading backup and disaster recovery solutions address this issue by leveraging advanced technologies such as screenshot verification, which automatically boots up a backup copy of a protected server as a virtual machine on the backup appliance, and takes a picture of that login screen so you know the server can be restored.

Ensuring your business has an appropriate backup and disaster recovery solution in place should be at the top of your to-do list. Avoid these common mistakes and seek the advice of an experienced provider to help you get there.

What Is the 3-2-1 Rule for Backup & Disaster Recovery?

The 3-2-1 backup rule is an easy-to-remember acronym for a common approach to keeping your data safe in almost any failure scenario. The rule is:

3 Keep at least **three** copies of your data.

2 Store **two** backup copies on different storage media.

1 **One** of those copies should be located offsite.

PART 5

Should Businesses Insource or Outsource Backup & Disaster Recovery?

Ultimately, companies have two options to address their backup and disaster recovery needs. They can take it on themselves or outsource it to a qualified managed services provider (MSP).

Why Should Your Business Outsource Backup & Disaster Recovery?

Organizations like yours outsource backup and disaster recovery instead of handling it in-house for these key reasons:

Lack of Expertise

The breadth and depth of knowledge demanded by IT teams today is vast and spans not only cybersecurity expertise but data storage, data integrity insight, software development, information technology infrastructure library (ITIL) knowledge, database design and management, network services, cloud computing, data analysis, troubleshooting and more. Security is a unique and complex discipline in of itself.

Lack of Time

Due to the interconnected nature of integrated applications, devices and other technologies, IT departments are stretched thin putting out fires. Many teams don't have the time to handle complex cybersecurity measures, like backup and disaster recovery, effectively.

Lack of Talent

The IT skills gap is a well-known challenge for businesses, especially SMBs, that cannot typically pay for hard-to-source expertise. This skills gap is prominent in the hyper-specialized realm of cybersecurity and backup and disaster recovery.

Common Challenges Managed Backups Help Solve:

A managed backup environment helps organizations overcome these common IT challenges:

- Limited Budgets
- Lack of Tools
- Hard-to-Retain Talent
- Limited Flexibility
- Resource Availability Challenges
- Skillset Gaps

PART 6

What Should You Look for in an MSP for Backup & Disaster Recovery?

Outsourcing backup and disaster recovery to a managed services provider (MSP) with security expertise is the most cost-effective choice for most businesses.

When seeking the right MSP to partner with, you must find one you can rely on to help you through all of your company's growth phases. That means top-tier expertise, financial stability, the size and reach to scale with your company as it grows, flexibility, reliability and 24/7/365 support.

What Capabilities Should Your MSP Deliver?

Key attributes to look for when selecting an MSP to manage your backup and disaster recovery include:

- **24/7 Monitoring —** True cybersecurity requires 24/7/365 management from a security operations center (SOC) staffed by security professionals. A 8/5/260 watch from a small provider won't cut it with today's threats.
- **Frequent & Regularly Tested Backups —** The MSP should test backups often in staging environments to ensure that when the time eventually comes, the BDR solution is deployed without issue.

- **Solid Technology —** Your MSP should have the infrastructure necessary to manage the solutions they provide. These include capital investments like security operations centers for managed security vendors, remote desktop access for instantaneous support and testing labs for testing firmware and software updates in staging environments before applying them to your live setup.
- **Clearly Defined Backup Strategy —** Does the MSP clearly explain where and how backups are stored to ensure data redundancy and protection? Have they outlined to your IT team what happens step-by-step in the event of needing to use the backup solution after a breach?
- **Clear Trouble-Ticketing System —** The MSP needs to provide a straight-forward way to access support from their technical team and quickly resolve any issues.
- **Regular IT Strategy Planning Meetings —** Your organization is expanding and changing and so will your IT strategy, including your BDR solution. Your MSP should regularly schedule quarterly meetings with your IT team to ensure solutions are still a fit and address any new requirements.
- **Easily Understandable Per Workstation, Per-Month Billing Structure —** A high-quality MSP offers standardized monthly pricing that is easy to scale and add or remove workstations as needed.
- **Remote Monitoring & Management (RMM) Agent —** Does the MSP offer RMM and do they use it internally on their own systems? Do they use some other software to implement the backup and disaster recovery solution?
- **Clear Service Level Agreement (SLA) —** What escalation paths does the MSP have available? Does the MSP offer your business a dashboard for your staff to view and see if SLAs are being met?

PART 7

Why Choose TPx for Backup & Disaster Recovery?

You have enough challenges in your business life. You don't need to worry about data breaches and the potentially catastrophic impact of ransomware on customer relations, business operations, workflow and your bottom line. At TPx, we have the products, services, experience and certifications to keep your network safe and running smoothly.

What Are the Key Features of TPx's Backup & Disaster Recovery Solution?

- **Hybrid On-Premises Backup Device & Cloud Backup Solution —** Our on-premises backup device includes replication and recovery to secure cloud environments for Windows, Linux, Mac & VMware systems.
- **Off-Site Retention of Backups to Cloud Environment —** Our solution eliminates the capacity thresholds of an on-site device and allows customers cloud storage options with unlimited amounts of data in the cloud for either a rolling 12-month period or the entire life of the account.
- **Backup Screenshot Verification —** Automated verification of successful backups where backups boot as virtual machines, capturing the login page, to prove your data has been successfully backed up.

Regular backups of your data can help you recover from a ransomware attack by allowing you to restore your systems and data from a safe copy.

- **Fast Failback Bare Metal Restore —** Perform a Bare Metal Restore from the snapshot of the original backup chain, while further backup operations continue.
- **Disaster Recovery Virtualization —** Ability to virtualize backed-up systems from on-premises backup device or from the cloud until on-site resources are restored.
- **Bandwidth Optimization —** Logical full backups only move incremental changes over the network, saving bandwidth utilization.
- **Device and Cloud Audit Reports —** Daily, weekly and monthly reporting on assets being backed up, backup jobs' success or failures, and screenshot backup verifications.
- **Ransomware Protection —** Scan of backups for detection of ransomware via analysis of the backup image.

What Are the Key Benefits of TPx's Backup & Disaster Recovery Solution?

- Improved Recovery Time Objective (RTO)
- Improved Recovery Point Objective (RPO)
- Enhanced Disaster Recovery
- Ransomware Protection
- Controls Costs
- Keeps Sensitive Data & Applications Safe
  - Reduces Exposure to Data Loss from Cyberattacks, Exploits, Malware, Human Error, System Failure & Natural Disasters
- Offers Proactive Monitoring
- Provides 24/7/365 Recovery & Restoration
- Minimizes Downtime
- Frees Internal IT Staff
  - No Managing or Monitoring from Internal Teams
- Protects Company Reputation, Clients, Profitability & Productivity

Backup & Disaster Recovery Services: What Will TPx Do?

When businesses outsource backup and disaster recovery to TPx, we handle:

- Backup Restore Assistance
- Configuration of Backup Jobs
- Managed Backup Administration
- Configuration of Ransomware Detection
- On-Site Troubleshooting Assistance
- Configuration of Exchange/SQL Aware Backups
- Ongoing Maintenance and Rapid Replace
- Self-Service Backup Administration
- Recovery of FILE/FOLDER from Backups
- Proactive Monitoring and Reporting for Backup Job Failures
- Reinitiate Backup Jobs in the Event of a Backup Job Failure

Why Choose TPx?

Our mission is being the easiest MSP to do business with

We solve the biggest IT issues — cybersecurity, connectivity, and collaboration — under one umbrella

We have 120+ certifications across 60+ competencies, like CompTIA, Cisco, Fortinet, AWS, SMC

We offer HIPAA, PCI-DSS, and SOC 2 Compliant solutions

We provide enterprise-class, 24/7 support

We offer different service levels and highly-customizable solutions

We have a national footprint with multisite, multi-carrier, partner coverage

With 18,000 clients in 49,000+ locations, we're big enough to get the job done and small enough to be agile

We have various dedicated teams to ensure service excellence

We continuously invest in automation, self-service innovation, and back-office transformation

We are committed to providing the most densely monitored service delivery platform in the industry

We understand and embrace the criticality of our customers' performance analytics

All-in-One Managed Services Portfolio Built for Your Business

Managed IT

Fully managed and co-hosted IT services that enhance performance, optimize networks and improve system stability. Our best-of-breed technologies, combined with our service expertise, keep critical IT systems operating smoothly. Join the thousands of companies that trust TPx to manage their IT infrastructure and get the peace of mind you deserve.

Managed Security

With cybersecurity threats growing in frequency and complexity, you need the right security in place to prevent, detect and stop cyber threats. TPx offers a multi-layered approach to security with best-in-class software backed by our highly trained security experts. Protect your business and keep your data secure with TPx.

Cloud Communications

Bringing people virtually together is easy with an intuitive, unified communications solution like UCx with Webex. It's a single app for calls, messaging, meetings, video, screen-sharing and more. Whether you're a small business, enterprise or call center, experience quality voice and unmatched collaboration capabilities with UCx.

PART 8

Glossary of Terms

Below are definitions of cybersecurity terms featured in this guide:

Backup: Copying data from a production system (Server/PC) to a separate storage location (Disk/Tape) so it is protected in the event of a disaster.

Restore: Copying backup data back onto a production system.

Disaster Recovery: Restoring all critical systems and data if disaster strikes (Cyberattack, Natural Disaster, System Failure, Human Error). Disaster Recovery focuses on getting technical operations back to normal in the shortest time possible.

Business Continuity: The processes and procedures that organizations take to make sure that regular business operations continue during a disaster. It includes Disaster Recovery and also things like: Who is essential personnel? Where will they work from? What systems will they use? What emergency processes are in place to conduct business? etc.

Disaster Recovery-as-a-Service (DRaaS): DRaaS delivers a suite of technology and services that allows an organization to recover and run failed systems in the cloud. Simply storing a backup copy in the cloud is not DRaaS but being able to initiate the failed servers from a backup copy as virtual machines (VMs) and run them in production from the cloud is.

Recovery Time Objective (RTO): The desired time in which a business needs to have a system back up and running before it too negatively impacts the business. For example, “I need to have this data and application available within four hours; otherwise, I start losing too much business and productivity.” In this case, the business’s RTO is four hours.

Recovery Point Objective (RPO): The RPO deals with the interval of time that passes between the last good backup and the point of a disaster. As an example, let's say a business backs up its data once each night at the end of the business day and they have a disaster at 4 p.m. today. The last good data is from yesterday, which means when they restore the operations, they will have lost 8 hours of data (8 a.m.-4 p.m.). If the business decides that losing 4 hours' worth of data would too negatively impact their business, then their RPO is 4 hours and the solution described here does not meet that objective.

Virtualization: Many backup and disaster recovery solutions now include the ability to run a virtual machine (VM) right on the backup infrastructure. As an example, if a production server that is being backed up to a local backup appliance experiences a failure, the backup appliance can recover a virtual instance of that server from a backup copy and that new VM runs right on the backup appliance and becomes the production machine. This allows the failed production server to be fixed offline, without affecting business operations.

Backup: The backup interval refers to the time span between backups. Older traditional systems based on legacy backup software and storage media, such as tapes, typically limit backup intervals to one time per day due to system performance limitations. Newer solutions can back up systems multiple times per day – often as frequently as every five minutes.

Retention Schedule: A retention schedule, or retention policy, refers to the length of time that backups are stored in a particular location, such as on the local target storage device, or on the offsite/cloud storage target. A typical local retention policy might be to keep backup data on the local device for 30-90 days. This makes it easier and quicker to recover the most recent data. Then, longer-term retention, which may be years, happens at the offsite/cloud location.

Ready to Take Charge of Your Backup & Disaster Recovery?

CONTACT US TODAY