Red River

WHY AZURE DISASTER RECOVERY

COULD BE CRITICAL TO YOUR ORGANIZATION

75% of businesses today don't have a disaster recovery plan. And that's a problem.

Modern businesses rely upon data for their most critical of operations. Companies have to pay their employees based on their HR solutions. They have to interface with customers through their CRM platform. They have to process purchase orders through their ERP. Without data, everything comes grinding to a halt. Despite that, many companies aren't paying attention to their backups.

It's not because companies don't care. For the most part, it's because these companies don't have the resources they need.

To maintain backups and a disaster recovery plan, companies have to pull their IT department off other tasks. They may need to sacrifice revenue-generating tasks, or they may need to pull their staff away from putting out other fires. Backups can seem like a trivial process until it becomes non-trivial. IT departments may let their backups and preparation slide until it's too late.

Azure Disaster Recovery can help.

Let's explore some of the major threats to data today and how Azure Disaster Recovery can be used to defeat them.

ORGANIZATIONS TODAY RELY UPON THEIR DATA — BUT IS IT SECURE?

- Despite companies today relying more upon data than ever, some companies still don't have a disaster recovery plan.

- Companies rely upon their data for almost all their operations and may be frozen and unable to operate without their information.

- Azure Disaster Recovery can help an organization maintain more consistent updates and a better disaster recovery process.

Companies are using more data. 49% of companies say that their data helps them make better decisions. From point-of-sale systems to customer relationship solutions, companies need their data to remain in operation.

But there are many threats that organizations may encounter:

- **Ransomware.** Ransomware frequently targets small and medium-sized businesses, encrypting the company's data and holding it until the ransom is paid. (And even then, paying the ransom is no guarantee your data will be – or even can be – restored. Even companies that have secured their network may still fall prey to ransomware due to the actions of an employee. But if a company already has its data backed up, it can simply restore it. Ransomware only works if the company has no other access to its data.

- **Overwriting.** When multiple employees are working on the same files, it becomes more possible that data can be accidentally deleted, overwritten or corrupted. The ability to restore data from backups means that the new work won't be lost. Instead, it can be restored with the click of a button. Multiple versions of files can be saved to the cloud for even greater levels of consistency.

- **Physical threats.** While many organizations are focused on defeating digital threats, they aren't the only types of threats out there. Physical damage can always occur. Someone can simply walk away with a hard drive rather than attempting to encrypt it. Companies have to be able to access and restore their data to protect against these types of threats.

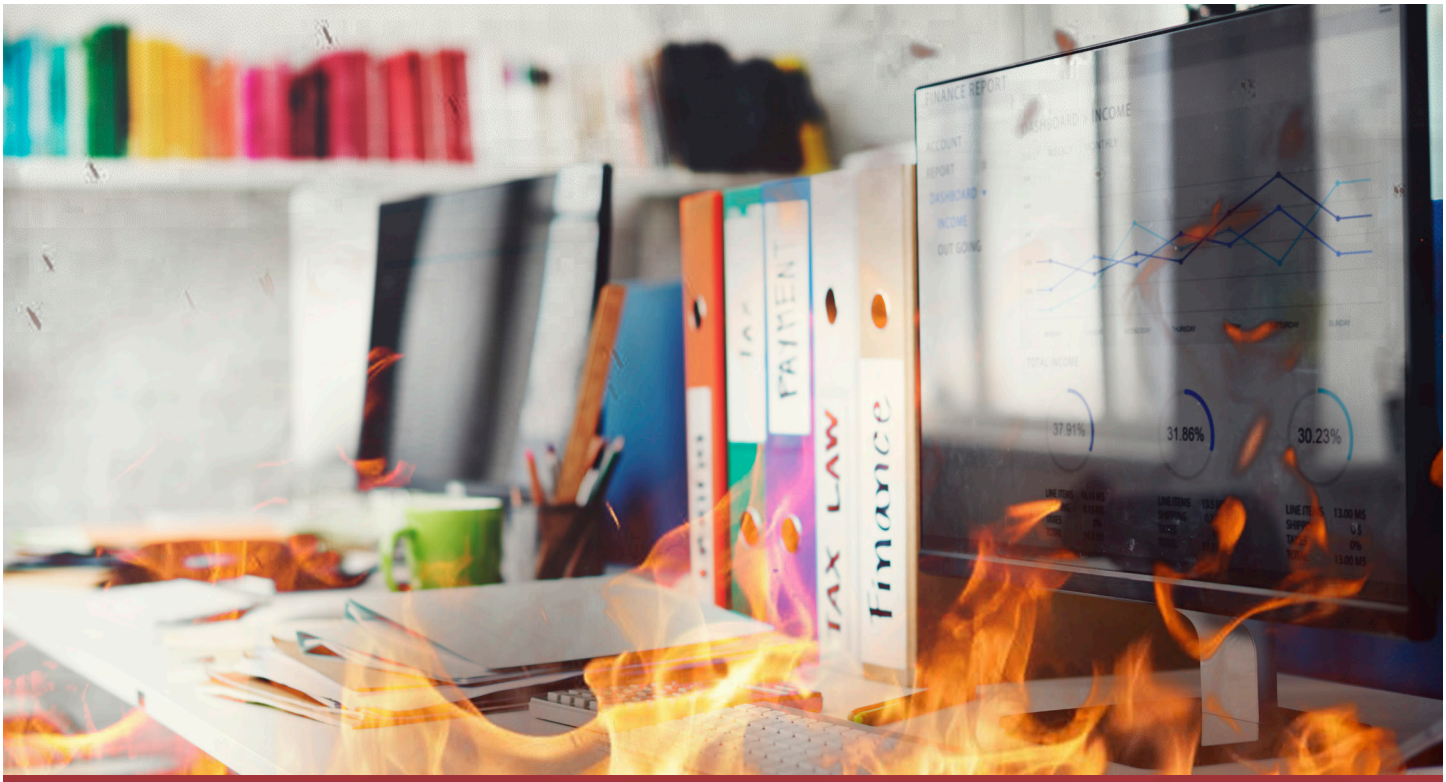
- **Data breaches.** Rather than the data being taken away, such as under ransomware, the data can simply be copied and distributed. Your organization may need to shut down to seal up the breach and it may have a long road ahead of it in terms of re-establishing client trust. Azure Disaster Recovery can help organizations who have experienced data breaches reset and protect their system.

When organizations don't have access to their data, they can't function. But many organizations aren't maintaining reliable backups simply because they haven't prioritized it. Backups are like insurance: You never need them until you do. Companies may not realize how flawed their backup and disaster recovery processes are until they've encountered an issue and by then, it's usually too late.

With as many threats as companies have today, it makes no sense not to plan for the future. An Azure Disaster Recovery program will help a business develop its backups, syncing and restorations based on what the business needs the most. Because every business is unique, it's frequently the case that an Azure Disaster Recovery program will need to be tailored to an organization.

Many companies will fold entirely after having a major data breach; even if it survives, the costs of a data breach are extensive. Not only can the company not operate while its technology is down, but data breaches also require notifying customers — which can lead to a loss of faith. With many companies working hard to ensure that they have loyal clientele, a loss of trust can be disastrous.

Key Takeaway: *Organizations are exceptionally reliant upon their data and they need a plan that will prevent their business from being disrupted.*



PHYSICAL DISASTER CAN OCCUR WHEN IT'S LEAST EXPECTED

- Not all data disasters start in the digital world; physical disasters are also very common.
- Backups should never be stored in the same place as the originals. Cloud solutions are typically ideal.
- Companies need to test out their physical disaster processes to ensure that they're safe.

Fires, floods, earthquakes — there are a tremendous number of physical disasters that can occur without any warning. Azure Disaster Recovery helps organizations protect themselves against these types of unexpected events.

Consider a fire. A company may have backups of their data to protect against ransomware attacks, but what if those backups are held within the same facility as the original copies? Now both original and backup could be damaged or lost. Many companies make the mistake of backing up their documents to the same geographical location as their originals. This exposes the company to a tremendous amount of vulnerability.

Today, many businesses are operating on the cloud and backups and syncing are also done through the cloud. This helps: If a physical disaster strikes, the data is still there. But if the cloud backups aren't current or are corrupted, the company is again at square one. While cloud-based backup solutions can help, they still need to be monitored and testing to ensure that they are operating properly.

Cloud-based solutions are more likely to be safe if they are through a reputable company such as Microsoft. There are many companies who have cloud-based solutions that aren't necessarily completely secure and companies need to do their own due diligence about which cloud-based solutions they can trust.

cloud-based platforms are more secure than on-premise platforms, primarily because the technology has changed and because of the way that the cloud works — it's able to deploy superior levels of resources, compared to companies with on-premise solutions.

At the end of the day, companies need to consider that they may be vulnerable to certain types of threat. And they need to operate to address these threats, rather than simply hoping that they won't occur. Modern backup solutions make it easy to "set and forget" the system, but forgetting is the operative word: It's easy to forget that disaster recovery is a necessity until the disaster has already occurred.

It should also be noted that many "Acts of God" aren't covered by insurance policies. Companies should take a look at what their disaster policies cover and should consider getting disaster recovery or business interruption insurance if they don't already have it. When your data is gone or corrupted and you need to ensure that your business survives, business insurance can frequently help.

Key Takeaway: *Disasters can occur both physically and digitally and it's absolutely essential that companies prepare for both eventualities. It isn't a matter of if, it's a matter of when.*

COMPANIES MUST MANAGE BOTH INTERNAL AND EXTERNAL THREATS

- A company's threats come from both outside and inside.
- Employees have to be managed correctly to reduce the potential for threat.
- All employees will eventually make mistakes, and no employee is perfect.

Companies aren't just managing threats from outside of themselves, such as criminal attackers and floods. Companies are also managing internal threats.

Employees can be internal threats for multiple reasons. In rare cases, there may be disgruntled employees who are trying to cause damage to the system. More commonly, an employee may simply make a mistake and accidentally damage files or make changes to the internal network. They may expose the business to a virus or other malware through their own curiosity.

Because employees need to deal with a large amount of data, they can be a vulnerability to the organization. And there's little that an organization can do about this directly: It's impossible to control employees or to ensure that they never make mistakes.

Instead, organizations must act to protect their data. Organizations need to back up their data on a regular basis, so that any mistakes made by employees won't be as damaging as it would be otherwise. And companies can reduce the amount of threat that their employees represent. Companies can offer frequent cybersecurity training seminars and regularly reinforce the idea for their employees that security is a paramount concern.

External threats are another big challenge: Companies need to be able to deal with criminal attackers, unexpected events and more. But companies can't anticipate these events: They can't know when an external threat will occur. Like an internal threat, companies need to deal with this by mitigating the amount they can potentially lose through an external threat, as they cannot remove the threat altogether.

Perhaps more importantly, many companies find that their IT departments simply don't have the time to regularly follow up on external and internal threats. Instead, IT departments need to rely upon managed service providers and other professionals to ensure that their security is well-managed. Platforms like Azure Disaster Recovery can put more power into the company's hands and they can be used through an MSP to provide both best-in-class technology alongside best-in-class customer support.

Key Takeaway: *Organizations must be aware of both their internal and external threats and take proactive action to prevent these issues from taking place.*

THE MAJOR BENEFITS OF AZURE DISASTER RECOVERY

There are many disaster recovery solutions out there. What makes Azure special? Azure Disaster Recovery has a number of benefits over traditional backup platforms, owing to its integration, advanced technology and robust feature set.

- **Unify your data management and protection.** Today, organizations are operating with complicated networks including a myriad of third-party solutions. While a company's core data may be protected, it's more than possible that it may have other sources of data, such as legacy solutions, that are not. Azure disaster recovery makes it possible to unify all data management and protection, thereby providing for a more consistent experience. Companies can rest assured that all their data is protected, not just some of it.

- **Test your disaster plan as needed.** Azure makes it possible to test your data restoration and disaster recovery processes, without affecting your end users. Too often, companies find that their disaster strategy doesn't work for the first time when they're trying to follow it. Disaster strategies should be tested and audited regularly; otherwise, you can't know whether your processes are reliable.

- **Restore your data with the click of a button.** Azure will sync your data automatically, alongside your applications and your infrastructure. If issues do arise, you can restore your data with the click of a button. You won't lose any time: You'll be able to hit the ground running again once your system has been restored. This can save companies thousands or even tens of thousands of dollars.

- **Integrate your disaster recovery with your existing solutions.** Azure Disaster Recovery is particularly useful for companies that are leaning on the Windows environment. The Windows environment integrates completely, creating an entire all-in-one ecosystem that's easy for users to use and easy for IT personnel to manage.

- **Don't worry about the downtime.** The ultimate end goal of Azure Disaster Recovery is to reduce your organization's downtime and protect your company's information. With Azure Disaster Recovery, you know that your organization will be able to re-deploy its information whenever it needs to. Your organization isn't going to have to worry about losing its data forever or spending days trying to reconstruct it. Instead, your company can focus on what it does best.

At the end of the day, a company's data is its most vital resource. But protecting this data can cost a company a prohibitive amount of time and energy. Through Azure Disaster Recovery, companies are able to protect their data and ensure its consistency.

Are you ready to find out more? Red River can help you with your Azure Disaster Recovery needs. Contact Red River today to schedule an appointment.

ABOUT RED RIVER

Red River brings together the ideal combination of talent, partners and products to disrupt the status quo in technology and drive success for business and government in ways previously unattainable. Red River serves organizations well beyond traditional technology integration, bringing 25 years of experience and mission-critical expertise in security, networking, analytics, collaboration, mobility and cloud solutions. To learn more, visit redriver.com.