Acronis

WHITE PAPER

Why your business needs a disaster recovery solution

Businesses face an evolving array of threats to their continuous operation, including natural disasters, tech infrastructure failures, human errors and cyberattacks.

As a result, disaster recovery (DR) has become an essential tool to protect businesses from cyberthreats, including ransomware attacks, serving as a pillar of business continuity and cybersecurity defense-in-depth strategies.

This white paper will examine the topic of DR: what it is, the many benefits it can provide for businesses, and best practices for evaluating and buying a DR solution.

Executive summary

By reading this white paper, you will discover:

Introduction

When it comes to data protection and continuity of operations, organizations in many different industries — including finance, legal, healthcare, public sector, retail and construction — need to have a DR plan. DR is critical for businesses that rely on technology infrastructure, as well as those that are susceptible to natural disasters or human error.

Here are the four leading sources of business tech infrastructure downtime:

1. Cyberattacks: Cyberattacks are becoming more sophisticated and targeted, and can have a devastating effect on businesses of all sizes. A DR solution can help you recover from ransomware incidents, technology supply-chain attacks and other types of cyberthreats.

2. Natural disasters: Even if your business is not in an area prone to natural disasters, you cannot predict when severe weather and its impact on critical infrastructure will affect your operations. A comprehensive DR solution will help you keep your business running in the event of a flood, blizzard, wildfire, earthquake or other disaster.

3. Technology infrastructure failure: Technology infrastructure failures can occur without warning and significantly affect business operations. A DR solution can help you recover from failures such as hardware or software crashes, power outages and network disruptions.

4. Human error: Human error is one of the most common causes of data loss and downtime. Whether it is an employee accidentally deleting critical files or misconfiguring a server, human errors are inevitable. In addition, the challenges of managing the rapid growth in remote work and cloud applications has driven up the potential for disruptive human errors. With a DR solution in place, you can minimize the impact of these errors on your business.

While no one likes to think about disasters, it is important for businesses to have a plan in place so that they can minimize the impact on their operations. A well-designed disaster recovery solution can make all the difference when it comes to getting a business up and running again after an unexpected event.

The adverse effects of downtime

When considering a DR solution, it is essential to consider the negative consequences of disrupted operations. Downtime can threaten a company's profitability, reputation, and even its viability. Some of the key impacts of downtime include the following:

Hard costs

- **Financial loss:** Downtime can result in lost revenue and increased expenses. For example, research shows that the proportion of outages costing over $100,000 has soared in recent years. Over 60% of failures result in at least $100,000 in total losses, up substantially from 39% in 2019.
- **Reduced productivity:** It could be difficult for employees to get their work done, leading to decreased productivity. For instance, if employees cannot work because of issues with computer systems, they may not be able to access files and complete their tasks.

Soft costs

- **Impact on customers:** Disrupted operations leading to delays in delivering products or services to customers. If a customer is trying to purchase something from your website and the transaction cannot be completed, they may become frustrated and take their business elsewhere.
- **Loss of reputation:** Downtime could lead to negative publicity, damaging the company's reputation and brand, making it more challenging to retain and attract new customers and partners. Your customers may go to your competitors if they cannot access your site.

Cyber insurance qualification

Disaster recovery may now be a prerequisite for many businesses to qualify for cyber insurance. In response to the ongoing surge in ransomware attacks, most cyber insurers have now imposed strict new requirements for cybersecurity and resilience capabilities on prospective policy holders that, if not met, can result in significantly higher premiums or outright denial of coverage.

Service level agreement breaches

A service level agreement (SLA) is a contract between a service provider and a customer that specifies the nature and quality of the service to be provided. Breaches of SLAs can occur when the service provider fails to meet agreed-upon standards like application availability or network uptime, resulting in disruptions or downtime for the customer and financial penalties for the provider.

Compliance fines and penalties

Businesses that are subject to industry or government regulation may face additional consequences of tech infrastructure downtime. For instance, any businesses that serve customers residing in the European Union fall under the scrutiny of its General Data Protection Regulation (GDPR) regime, which can assess financial penalties to businesses that fail to protect or provide customer access to sensitive personal data. USA-

based healthcare providers face their own set of privacy protection and customer data access regulations under Health Insurance Portability and Accountability (HIPAA) Act. If these standards are not met, your business may face financial penalties, lawsuits or other sanctions.

What is disaster recovery, and how does it work?

In disaster recovery (DR), business-critical data and applications are replicated in an off-premises location, such as a cloud-based environment, that is expected to be unaffected by a localized cyberattack or natural disaster. For example, if a business's local servers fail due to a hurricane, equipment failure, or ransomware attack, workers may resume business operations by accessing copies of their applications and data that have been backed up to the cloud. When the DR has been restored, workers can then be switched back to their original applications and data. DR solutions help organizations maintain business continuity and minimize the impact of downtime and data loss.

Benefits of implementing a DR plan

An IT disaster recovery plan outlines the policies, procedures and responsibilities for failing over to replicated standby resources in the event of a disaster, so that business operations can resume as quickly as possible. A DR plan should be regularly tested to ensure the organization's IT systems can smoothly switch over to standby systems when a disaster occurs, then back again once the original site has been restored.

Some key benefits of DR planning include:

- **Reduced downtime:** By having a comprehensive DR strategy in place, your business can resume operations quickly and safely in the event of a disaster.
- **Lower financial impact of disasters:** A DR plan can limit legal liabilities, losses, compliance sanctions and other damages resulting from a disaster.
- **Increased satisfaction and lower reputational impact:** Having a reliable DR plan can improve employee, partner and customer satisfaction and trust in the business.
- **Peace of mind:** Businesses can know that their data is protected and that their operations can get back up and running as quickly as possible after a disaster.

Best practices to consider when evaluating disaster recovery solutions

Business-critical data is stored in multiple ways: in a data center, in an off-site physical location, in a private, public or hybrid cloud environment, or in some combination of these options.

Your production applications and data in your primary site or data center are considered your first copy. Businesses commonly store backup copies

Disaster recovery has become an essential tool to protect businesses from the existential threat of ransomware attacks, serving as a pillar of business continuity and cybersecurity defense-in-depth strategies. Disaster recovery enables businesses to greatly improve their chances of surviving a ransomware incident. In the event of an attack, businesses can quickly switch operations from production applications under attack to standby copies in the cloud, switching back to their primary infrastructure when the attack has been terminated and mitigated.

Why haven't many companies invested in disaster recovery?

Historically, businesses in the medium-size to midmarket segment (100 to 2,000 employees, with a small to nonexistent internal IT staff) have avoided investing in DR solutions, believing them to be too complicated and expensive. The emergence of externally managed, cloud-based solutions has made DR much more affordable and less complex for these smaller companies.

of critical applications and data in a separate physical location relatively close to the primary production site. This option is comparatively inexpensive but can require days or weeks to conduct restoral operations. Some large enterprises with very high availability requirements may fully replicate their data center infrastructure, applications and data for rapid failover in the event of a major downtime incident, though this option is too costly for most businesses. A growing number of businesses also replicate key apps and data in cloud infrastructure, which is generally more cost effective, flexible, and remote or distributed enough not to be vulnerable to incidents that are localized to a business's primary location.

When it comes to protecting businesses from the devastating effects of a natural disaster, infrastructure failure or cyberattack, there are many solutions on the market. The best approach depends on the specific needs of each business. However, some key factors should be considered when evaluating a DR solution.

Why more businesses are moving to cloud-based DR

Businesses should consider a range of failover options for their DR strategy, including off-site physical locations and cloud services to maintain flexibility in recovery options and scalability as the business grows. Cloud-based services allow you to leverage cloud resources to replicate critical data and applications and rapidly switch over to the replicated environment in the wake of a disaster. The cloud-based approach generally offers lower operating costs, greatly reduced capital expenditures, and decreased operational management burdens than building and managing physical resources for DR purposes. Cloud DR also enables application and data replication across multiple locations for added protection and flexibility.

About Acronis Disaster Recovery

Acronis Disaster Recovery is a complete turnkey solution that is easy to implement and protects organizations against data loss and downtime from a single console. It provides automated, secure and cost-effective protection for physical and virtual networks, applications and data.

Acronis is the answer to help you meet your immediate data recovery needs — with out-of-the-box recovery time objectives (RTOs) and recovery point objectives (RPOs) of under a minute to an optional automated cloud-based DR implementation for critical apps.

- **Predictable and dependable business continuity:** Minimize business impact and achieve the fastest recovery from a disaster or cyberattack, including ransomware.
- **Malware and vulnerability-free recovery:** Scan backups for vulnerabilities and malware, remediating them before restoration to ensure clean recovery.
- **Flexibility:** Easily and quickly recover systems from any platform (hardware, virtual machine, or cloud environment) to a matching or completely different platform.
- **Real-time threat feeds:** Get dynamic, real-time threat alerts relevant to your environment to help prioritize threat response and mitigation actions.

Conclusion

Selecting the right DR solution is a complex process that requires careful consideration. There are several steps to review before choosing your DR solution: from defining your requirements and evaluating existing solutions to creating an implementation plan, regularly testing it, and executing it as efficiently as possible. By having a plan in place, you can ensure that your chosen DR strategy not only meets all your needs, but has the flexibility to adapt to future disasters.

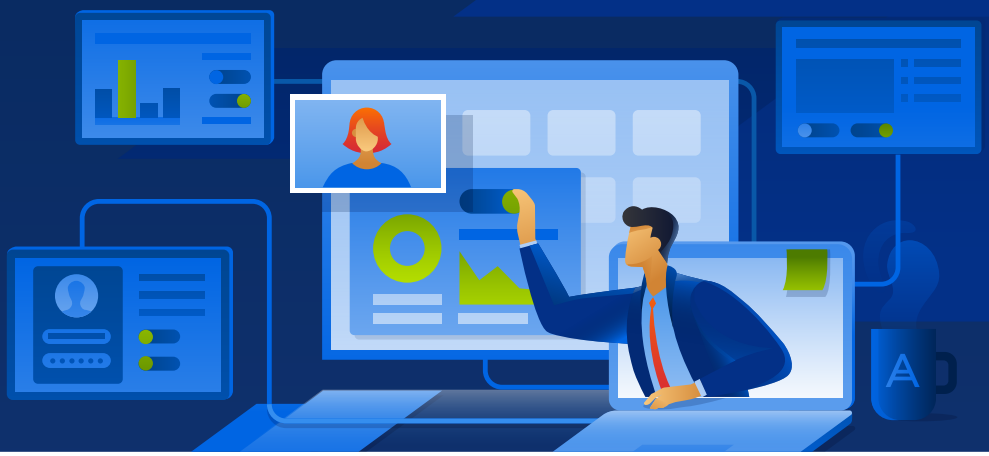
Cloud DR solutions are a valuable tool for protecting your data and ensuring business continuity in an emergency. When deciding which solution to buy, consider such factors as cost, scalability, ease of use, and other features that can help you achieve your goals. With the right solution, you can quickly recover from any disaster situation with minimal disruption.

Find out how Acronis Disaster Recovery can effectively protect your business against data loss and downtime. You can also set up a free call with one of our solutions engineers for further help.

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore and headquartered in Switzerland, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.



Acronis

Learn more at
www.acronis.com