Acronis

#CyberFit

The Secret Shortcut to Disaster Recovery

Table of contents

Introduction

You may believe that backup is enough. You may not understand how valuable your data, systems, and applications are until they're compromised. Disaster recovery is that necessary extra step to get up and running again quickly after an outage.
We know, it will never happen to you. It's only a nice-to-have.

What is disaster recovery?

Disaster recovery (DR) won't work without backup. DR includes the most recent copies of data and processing capabilities in a platform that delivers automated availability of your most critical data, systems, and applications.

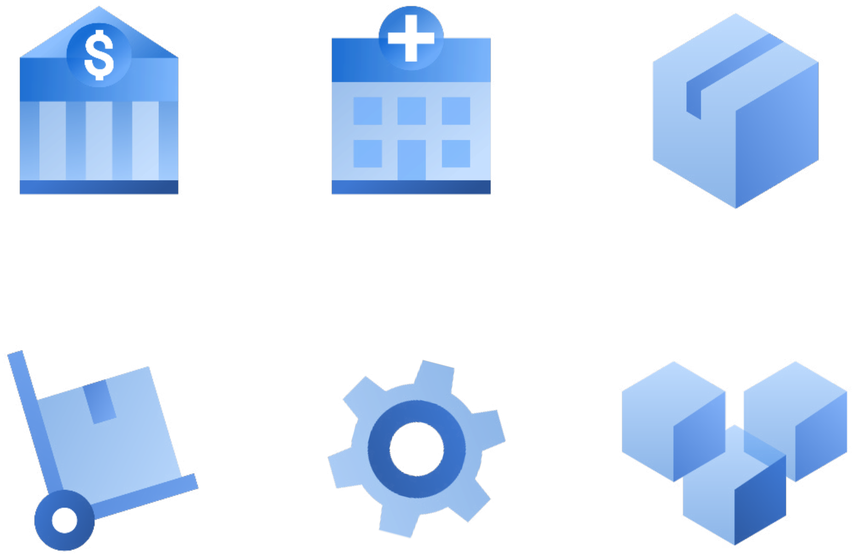
It ensures that interdependent processes are recovered in the correct order, restored to the correct recovery point, and in the right time.

Is your business ready?

Who needs DRaaS? Everyone. Any business can fall prey to disasters. You might be located in disaster-prone areas or lack the technical resources or necessary experience to implement a disaster recovery program.

Industries like these rely on mission-critical applications and data or face heavy regulatory and compliance fines:

- Financial Services
- Healthcare
- Legal
- Transportation
- Telecommunications
- Manufacturing
- Construction
- Energy
- eCommerce
- Utilities
- Supply Chain and Logistics



It's not just IT

Getting back to business fast isn't just an IT issue. When outages affect Human Resources, Finance, Legal, and other departments, it's everyone's problem.

IT

- Backup and recovery
- SLAs, internal and external
- Employee satisfaction
- Audits
- Compliance and regulations

C-Suite

- Business continuity plans
- Market perception
- Employee productivity
- Compliance and regulations
- Insurance

Finance

- Compliance and regulations
- Protection of sensitive data
- Maintaining business operations
- Market and economic confidence
- Audits

Human Resources

- Staffing and workforce planning
- Training
- Employee productivity
- Protection of sensitive data

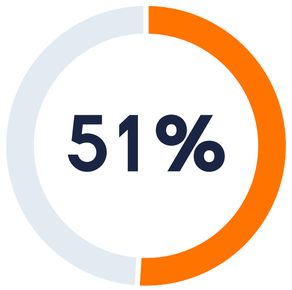
Legal

- Compliance and regulations
- Protection of sensitive data
- Insurance

The reality

Disaster can strike at any time, in various ways. We're here to stop you from becoming a statistic.

of data breaches in 2019 were caused by accidentally deleting or overwriting files or folders[1]



of data breaches in 2019 were caused by criminal and malicious attacks[1]

of organizations are likely to suffer business disruption by 2022 due to unrecoverable data loss[2]

of businesses experienced attacks within the past three years[3]

2.2 days

average length of downtime[2]

$5,600

average cost per minute[2]

$3.92M

average total cost of a data breach[2]

1) Ponemon Institute, 2019. 2) Gartner, 2019. 3) IDC, 2019

The threats

Which threats should you consider? You may believe that only natural disasters cause downtime with power outages that affect hardware. But software and people must also be considered. As technology develops, so too do the internal and external threats.

Natural disasters

Hurricanes, tornados, and fire can cause serious downtime by affecting facilities and infrastructure.

What most companies may not understand is that only 6% of outages are caused by natural disasters.

Pandemics

This type of threat affects an organization's people and, in the case of remote work, creates a whole host of planning scenarios IT departments may not have previously considered.

There is a greater risk when data and devices live outside of IT's regular infrastructure.

Hardware failure and software corruption

Hardware failure can be caused by a power outage. Software may become corrupt due to failed software updates, incorrect formatting of drives.

Human error with or without malicious intent

It happens. Many of us have accidentally deleted or overwritten something we didn't mean to.

A disgruntled employee might also wreak havoc with data and systems.

Cyberattacks

If even one employee's machine is compromised, entire networks can become vulnerable.

Attacks can happen quite quickly with weak passwords, falling for phishing scams, and clicking on malicious links.

Disaster recovery has evolved

1990s

Company data center or co-location cage

- Depreciated hardware
- Networking
- Licensing
- Replication platforms
- Massive amounts of storage

2000s

Hybrid approach

- Costly licensing
- Complicated
- Limited coverage

2010s

Modern hybrid and cloud-based DR

- Cost-effective
- Ease-of-use
- Ready-made

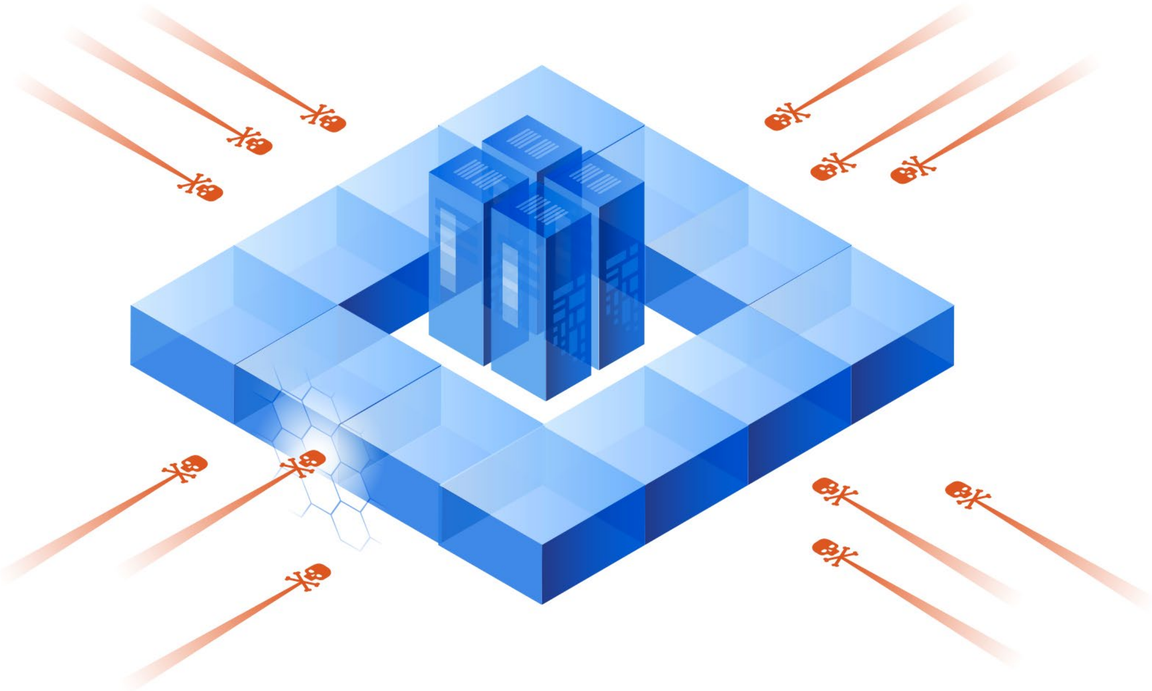
10 reasons you need to invest in disaster recovery

There are many reasons to go beyond backup with disaster recovery.

- Far more **cost-effective** than ever before
- **Minimize the impact** of any disaster
- Ensure continuous **employee productivity**
- Meet your **compliance and regulatory** requirements
- Access **instant recovery**
- **Reduce downtime** of operations
- **Reduce** potential **financial losses**
- **Reduce liability** obligations
- **Minimize the risk** of negative exposure
- **Facilitate** crisis management

Given the variety of internal and external factors that can affect your systems and data...

It is not a question of if you will experience data loss, but rather when it will happen.



Calculate the cost of downtime

These factors can be applied to your organization, using costs and numbers from all of your departments to calculate your actual downtime cost per hour. Bottom line? Downtime risks losing big money.

Lost revenue + Lost productivity + Cost to recover + Intangible costs = Downtime cost (per hour)

Lost Revenue

This is fairly easy to comprehend. If your business is down, you cannot generate revenue.

Use the gross annual revenue to calculate the amount of revenue per hour that is lost during downtime for each business area.

Lost Productivity

The cost of downtime also increases when your employees are unable to work or are forced to perform non revenue-related activities. Salaries or hourly wages are a fixed cost and must be paid regardless of how productive the employees are.

Cost to Recover

Often, you don't think about the costs associated with recovery and resuming normal business operations. Typical costs include:

- Services and employee time required to recover lost data
- Physical tools/devices that may need repair or replacement
- Cost of lost data

Intangible costs

Any damage to reputation or brand results in dollars lost. The slightest downtime can cast an insurmountable shadow over your business – and how that downtime is handled can be the difference between recovering and going under.

Paths to a DR program

When you manage your own disaster recovery program, you will need:

- **Staff for:**
  - Assessments
  - Design
  - Testing
  - Implementation
  - Management
- **Training**
- **Documentation**
- **Reporting**
- **Recovery Infrastructure**

If you choose a certified Acronis partner you will have:

- **Our years of disaster recovery expertise**
- **Rapidly and easily enabled disaster recovery services**
- **Ongoing and efficient delivery model**
- **24/7 support**
- **Simplified testing capabilities**
- **Monitoring and management**
- **Integrated cloud storage and compute resources**
- **Cost effective operational expenses**

Staying open for business has never been easier

Imagine a Single Agent. Single Console. Single Cloud.

Data Protection

+

Cybersecurity

+

Disaster Recovery

Backup and Restore

Primary focus:

- Prevent the loss of valuable data
- Data located on servers, workstations, and mobile devices

Endpoint Management and Security

Primary focus:

- Detection and deflection of malware attacks
- Vulnerability assessment and configuration management
- URL filter
- Patch management

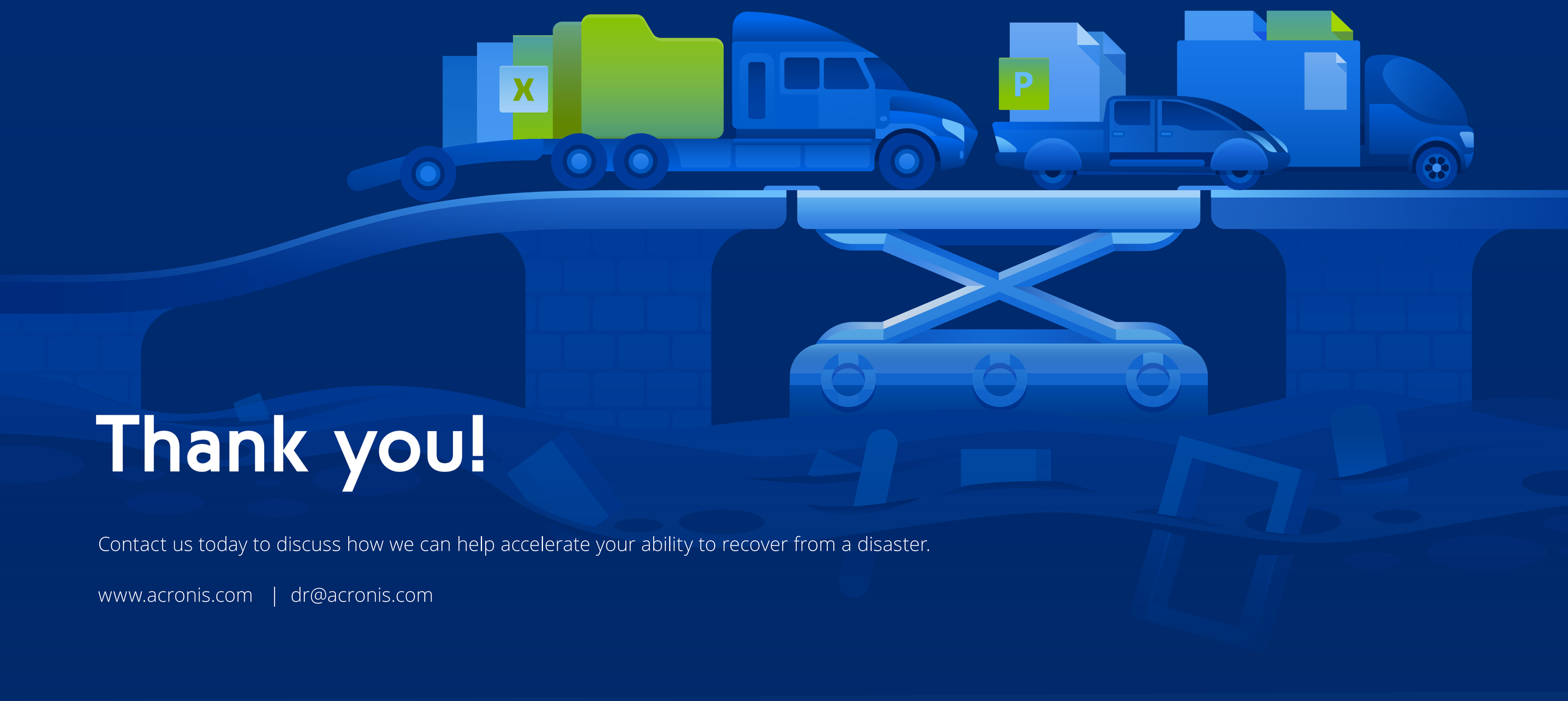
Disaster Recovery

Primary focus:

- High availability of critical applications
- Rapid recovery to avoid costly downtime

Acronis

#CyberFit



Thank you!

Contact us today to discuss how we can help accelerate your ability to recover from a disaster.

www.acronis.com | dr@acronis.com