Acronis

How to Sell Disaster Recovery Services

An MSP's DR Playbook

Table of contents

Introduction

Some of your SMB clients may believe that backup is enough. They also don't understand how valuable their data, systems, and applications are until they're compromised. Disaster recovery is that necessary extra step for you to get clients quickly up and running again after an outage. It can be a tough sell.
It's hard to have a conversation about potential threats when
a client thinks it will never happen to them.

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 clients' 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.

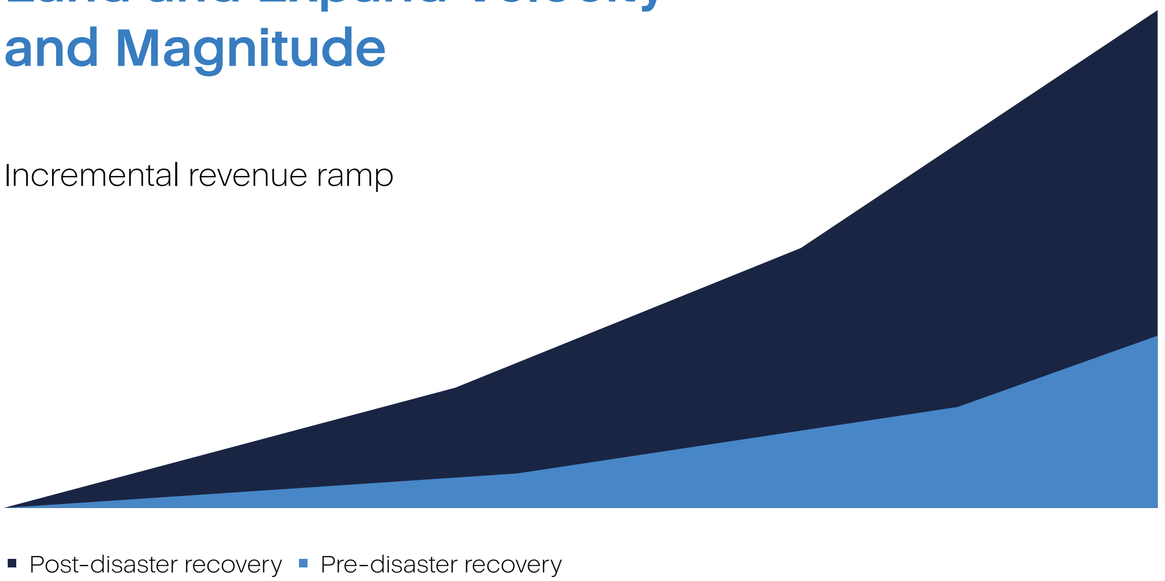
Forward-thinking MSPs grow revenue with DRaaS

As the saying goes, it's easier to sell to an existing client. You are 60-70% likely to sell to an existing client, compared to the 5-20% likelihood of selling to a new prospect. That means if you aren't cross-selling and upselling disaster recovery, you're leaving money on the table. Use your existing client data to increase revenue and commissions.

- DRaaS is cost-efficient
- Start immediately without having to add, learn, or manage another platform
- Gain better competitive positioning
- Deepen client relationships
- Increase client retention by creating more value from backed up data
- Improve the average revenue per user

Land and Expand Velocity and Magnitude

Incremental revenue ramp



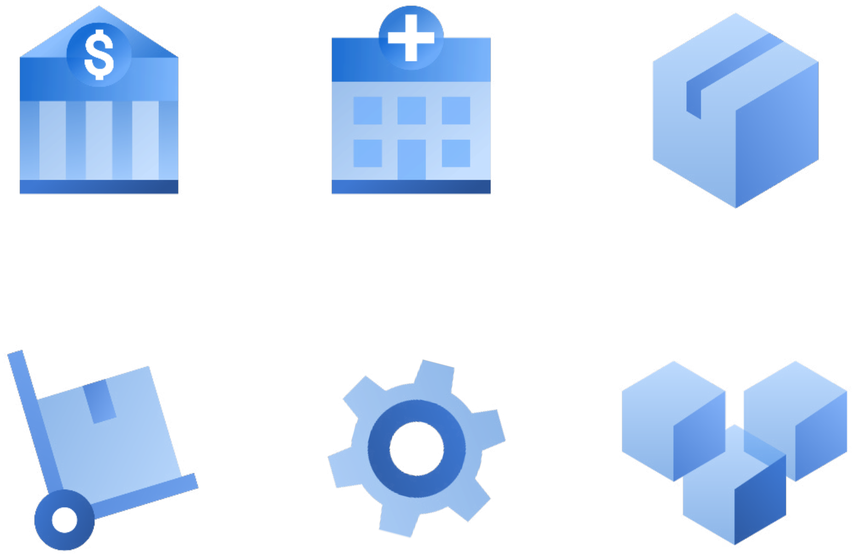
Target customer profile

Who needs DRaaS? Everyone. Any business can fall prey to disasters. Some clients may be located in disaster-prone areas, while others may lack the technical resources or necessary experience to implement a disaster recovery program.

Target verticals

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



How to position DR

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. Tailor the conversation to the different roles and responsibilities.

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

Common objections

Disaster recovery is most often seen as a "nice to have" instead of a "must-have." You may hear many reasons why disaster recovery is not on a client's radar, like these.

- **It's too expensive.**
- **It's too complicated.**
- **It won't happen to me.**

Handle these objections with the truth about DR from the following pages: the statistical reality, the types of threats, why they should invest in the "insurance" of DR, and what the actual cost of their downtime is. Quantifying the cost of disaster recovery (DR) against the costs of the inability to continue with day-to-day business operations will help to garner support for DRaaS.

The reality

Dispelling the "that'll never happen to us" thinking is easier when clients know the real numbers.

of organizations reported unplanned downtime[1]

of DR responses were triggered by software failure[1]

of organizations have suffered a data-related business disruption during the past 12 months[1]

of organizations experienced unrecoverable data within the past 12 months[3]

20 days

average length of downtime[2]

$22,000

average cost per minute[2]

$4.32M

average total cost of a data breach[2]

1) IDC, 2022. 2) Statista, 2022. 3) Forbes, 2022.

The threats

Describe the threats your client should consider. A client 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.

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.

Natural disasters

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

What most clients 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.

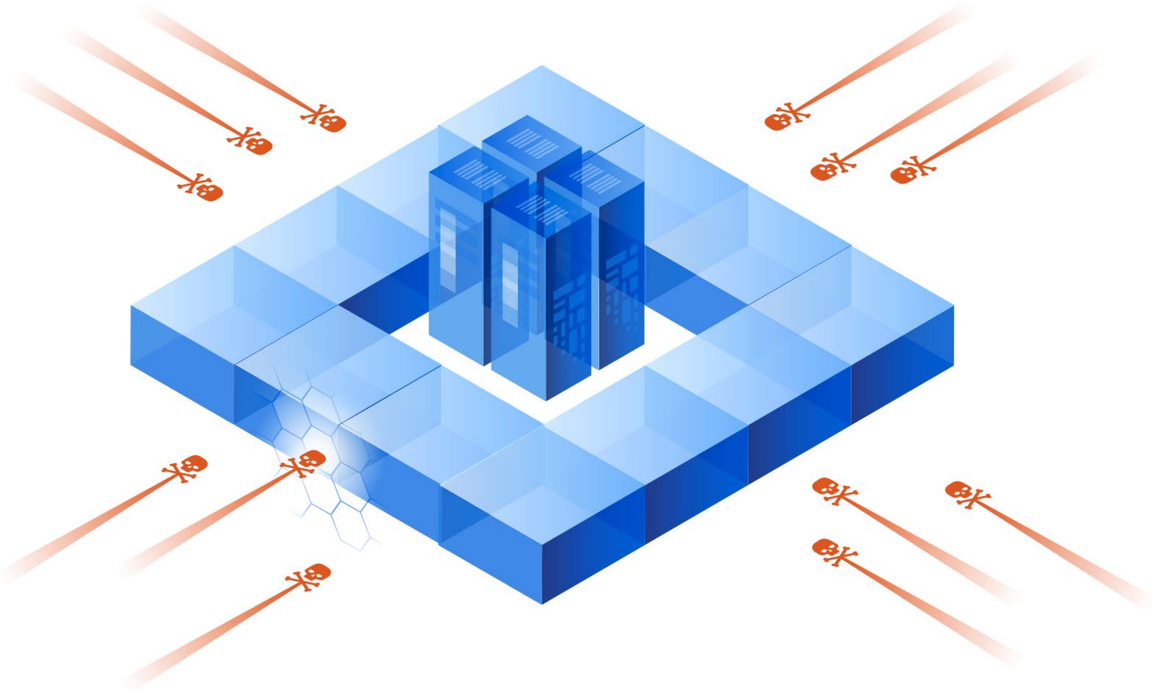
Human error with or without malicious intent

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.

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

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



10 reasons your client needs to invest in disaster recovery

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

- **Minimize the impact** of any disaster
- Ensure continuous **employee productivity**
- Become far more **cost-effective**
- **Meet compliance and regulatory requests** from your clients' financial, legal, and health industries
- Access **instant recovery**
- **Reduce downtime** of operations
- **Reduce** potential **financial losses**
- **Reduce liability** obligations
- **Minimize the risk** of negative exposure
- **Facilitate** crisis management

How to justify the incremental investment for total DR

It's easier than you think to increase your revenue, while saving time and money for your clients. The key advantage of cloud DR is that most of the expenditure is considered operating expenses (OPEX) rather than capital expenses (CAPEX).

It also saves IT significant time by eliminating the need to acquire, configure, test, and deploy servers that would typically sit idle.

Further benefits of a cloud DR solution are ease of use, agility, rapid recovery, and peace of mind. No need for an additional data center or machines.

Acronis Cyber Protect Cloud with Advanced Disaster Recovery makes offering DR services easy.

You have all of the ingredients. Just turn it on.

Calculate the cost of downtime

These factors can be applied to your clients' organizations, using costs and numbers from all of their departments to calculate their 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 client's business is down, they 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 clients' 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, clients 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

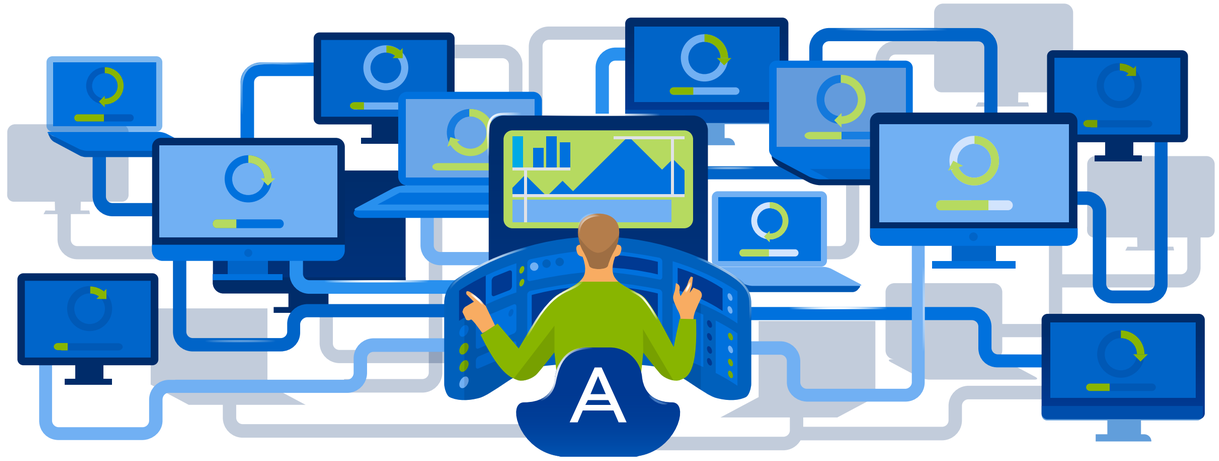
Intangible costs

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

Offer additional managed services with DR

A managed disaster recovery offering doesn't stop with the flip of a switch. For increased monthly, quarterly, or annual billings, offer your clients these additional managed services:

- Employee disaster preparation
- Pre-, during-, and post- workflow process mapping
- Off-site desktop, call center, and emergency command center
- Documentation
- Training
- Maintenance and upgrades
- Testing
- Reporting
- Audit support

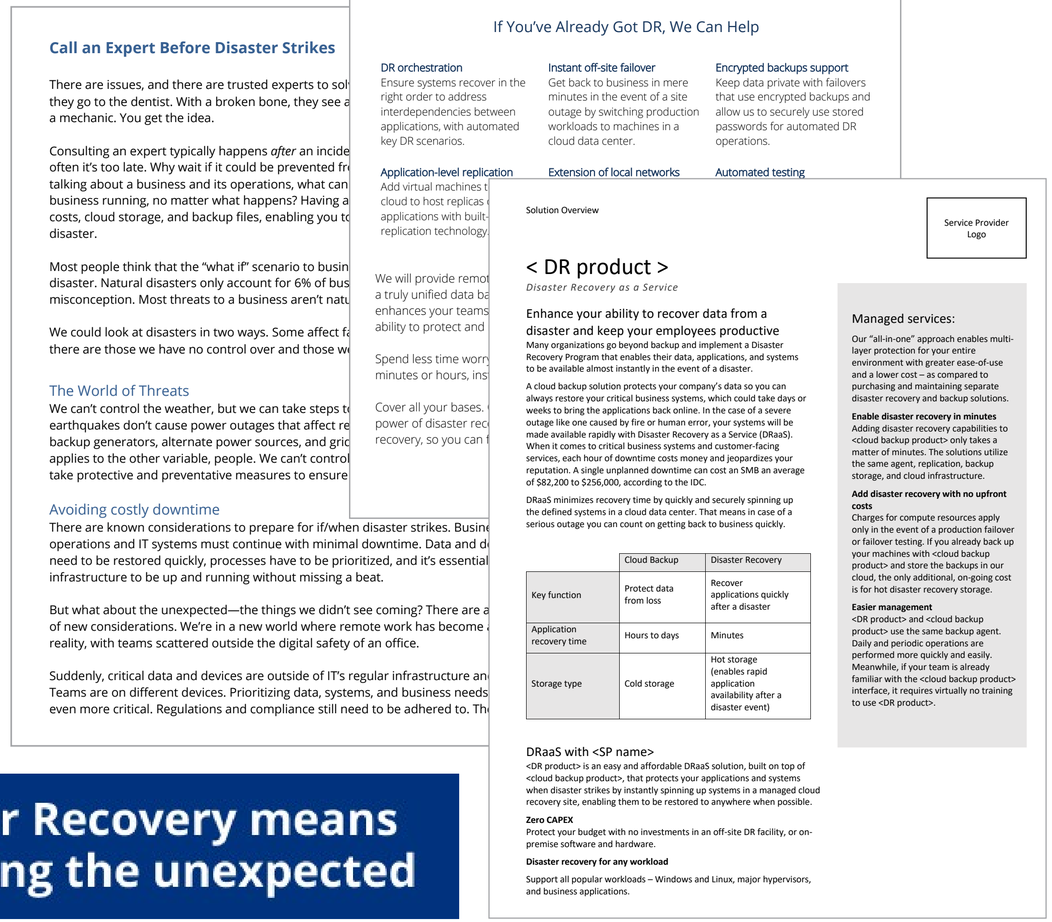


If you want to deliver a more fully managed experience, but don't have the expertise, there are Acronis partners available whose expert disaster recovery services can be white labeled.

Marketing resources

We've got everything you need to get started – easily white-labeled so you can customize materials with your logo and product names – conveniently located in the Acronis Partner Portal:

- DRaaS website page
- DRaaS blog post
- Datasheet
- Multi-touch email campaign
- Banners
- Easy-to-follow instructions



	Backup	Disaster Recovery
Key Function	Protect business from data loss	Minimizes downtime of vital applications and systems
Application Recovery and Data Loss	Hours to Days to Weeks	Minutes to Hours
Storage Type	Cold (physical)	Hot (cloud)

If You've Already Got DR, We Can Help

DR orchestration
Ensure systems recover in the right order to address interdependencies between applications, with automated key DR scenarios.

Instant off-site failover
Get back to business in mere minutes in the event of a site outage by switching production workloads to machines in a cloud data center.

Encrypted backups support
Keep data private with failovers that use encrypted backups and allow us to securely use stored passwords for automated DR operations.

Application-level replication
Add virtual machines t
cloud to host replicas
applications with built-
replication technology.

Extension of local networks

Automated testing

Call an Expert Before Disaster Strikes

There are issues, and there are trusted experts to sol
they go to the dentist. With a broken bone, they see a
a mechanic. You get the idea.

Consulting an expert typically happens *after* an incide
often it's too late. Why wait if it could be prevented fr
talking about a business and its operations, what can
business running, no matter what happens? Having a
costs, cloud storage, and backup files, enabling you to
disaster.

Most people think that the "what if" scenario to busin
disaster. Natural disasters only account for 6% of bus
misconception. Most threats to a business aren't natu

We could look at disasters in two ways. Some affect fa
there are those we have no control over and those we

The World of Threats

We can't control the weather, but we can take steps t
earthquakes don't cause power outages that affect re
backup generators, alternate power sources, and gric
applies to the other variable, people. We can't control
take protective and preventative measures to ensure

We will provide remot
a truly unified data ba
enhances your teams
ability to protect and

Spend less time worry
minutes or hours, ins

Cover all your bases.
power of disaster rec
recovery, so you can f

Avoiding costly downtime

There are known considerations to prepare for if/when disaster strikes. Busine
operations and IT systems must continue with minimal downtime. Data and d
need to be restored quickly, processes have to be prioritized, and it's essential
infrastructure to be up and running without missing a beat.

But what about the unexpected—the things we didn't see coming? There are a
of new considerations. We're in a new world where remote work has become
reality, with teams scattered outside the digital safety of an office.

Suddenly, critical data and devices are outside of IT's regular infrastructure an
Teams are on different devices. Prioritizing data, systems, and business needs
even more critical. Regulations and compliance still need to be adhered to. Th

Solution Overview

Service Provider Logo

< DR product >

Disaster Recovery as a Service

Enhance your ability to recover data from a disaster and keep your employees productive

Many organizations go beyond backup and implement a Disaster Recovery Program that enables their data, applications, and systems to be available almost instantly in the event of a disaster.

A cloud backup solution protects your company's data so you can always restore your critical business systems, which could take days or weeks to bring the applications back online. In the case of a severe outage like one caused by fire or human error, your systems will be made available rapidly with Disaster Recovery as a Service (DRaaS). When it comes to critical business systems and customer-facing services, each hour of downtime costs money and jeopardizes your reputation. A single unplanned downtime can cost an SMB an average of $82,200 to $256,000, according to the IDC.

DRaaS minimizes recovery time by quickly and securely spinning up the defined systems in a cloud data center. That means in case of a serious outage you can count on getting back to business quickly.

	Cloud Backup	Disaster Recovery
Key function	Protect data from loss	Recover applications quickly after a disaster
Application recovery time	Hours to days	Minutes
Storage type	Cold storage	Hot storage (enables rapid application availability after a disaster event)

DRaaS with <SP name>

<DR product> is an easy and affordable DRaaS solution, built on top of <cloud backup product>, that protects your applications and systems when disaster strikes by instantly spinning up systems in a managed cloud recovery site, enabling them to be restored to anywhere when possible.

Zero CAPEX
Protect your budget with no investments in an off-site DR facility, or on-premise software and hardware.

Disaster recovery for any workload

Support all popular workloads – Windows and Linux, major hypervisors, and business applications.

Managed services:

Our "all-in-one" approach enables multi-layer protection for your entire environment with greater ease-of-use and a lower cost – as compared to purchasing and maintaining separate disaster recovery and backup solutions.

Enable disaster recovery in minutes
Adding disaster recovery capabilities to <cloud backup product> only takes a matter of minutes. The solutions utilize the same agent, replication, backup storage, and cloud infrastructure.

Add disaster recovery with no upfront costs
Charges for compute resources apply only in the event of a production failover or failover testing. If you already back up your machines with <cloud backup product> and store the backups in our cloud, the only additional, on-going cost is for hot disaster recovery storage.

Easier management
<DR product> and <cloud backup product> use the same backup agent. Daily and periodic operations are performed more quickly and easily. Meanwhile, if your team is already familiar with the <cloud backup product> interface, it requires virtually no training to use <DR product>.

Other resources

From tech industry analysts

- Gartner: Acronis DRaaS Earns Gartner Peer Insights Customers' Choice and Singled Out in the "Voice of the Customer" Report"
- Frost & Sullivan: 2020 North American Data Protection New Product Innovation Award
- DCIG: Top 5 All-in-One DRaaS Solution Profile

From Acronis

- Partner portal: partners.acronis.com/en-us/profile/login.html
- Resource Center: www.acronis.com/resource-center
- Blog: www.acronis.com/blog
- Free trial of Acronis Cyber Protect Cloud: https://www.acronis.com/en-us/products/cloud/trial/#/registration
- Schedule a 1-on-1 demo or consultation. Email us at sp@acronis.com

Acronis

Contact your account manager today to discuss how we can help accelerate your ability to provide disaster recovery services.

Learn more at www.acronis.com