AN MSP'S GUIDE TO SELLING DR SERVICES

SCALE COMPUTING

Your clients might think having daily backups of their data, systems, and applications is enough. It's the old adage, "You don't know what you've got 'til it's gone." It's in situations like that where disaster recovery (DR) planning and overall evaluation of strategies is a valuable service you can offer.

But when those same clients think it'll never happen to them, how do you sell them this service?

It's important for them to know that backups are just a portion of what a BCDR plan is—That it's a holistic approach to bringing their production systems back online in a methodical way, in the right way, at the right time.

6 Ways Forward-thinking MSPs Grow Revenue with BCDR Planning

Capitalizing on existing client relationships through these strategies can yield substantial returns and foster sustainable growth in revenue and commissions. Additionally, bringing to light inherent risks that the clients may encounter will solidify those relationships and foster growth between companies.

1. Cost-efficiency
2. Get a competitive edge
3. Strengthen client relationships
4. Increase client retention by delivering more value
5. Drive higher average revenue per user
6. Reduce potential risk of loss to the client

Target Customer

Who can benefit from BCDR Planning? **Everyone.** Every business is susceptible to disasters in some form - from data loss to site outages, all businesses are at risk of some type of organizational downtime. Some clients might operate in regions prone to disasters, while others could face challenges in terms of technical capabilities or expertise required to establish a comprehensive disaster recovery initiative.

The following sectors depend on mission-critical applications and data or need to adhere to various types of regulatory or security compliance by industry, local, or federal governments:

- Financial Services
- Healthcare
- Legal
- Transportation
- E911
- Telecommunications
- Manufacturing
- Construction
- Energy
- eCommerce
- Utilities
- Supply Chain and
- Logistics
- Technology Providers
- Field Services Providers

Positioning BCDR

Different roles have different responsibilities and face different challenges. Know the customer and tailor the conversation to their business challenges.

C-SUITE

- Reactive in the aftermath of a disaster and the breakdown of business continuity initiatives
- Employee efficiency
- Industry, market, and customer perspectives and responses
- Adhering to compliance and regulations
- Insurance concerns
- Confident leadership in the face of adversity

IT

- Accountable for data backup and recovery
- Upholding SLAs, both internal and external
- Ensuring employee satisfaction
- Conducting audits
- Adhering to compliance and regulations
- Following the 3-2-1 rule
- Invoking and validating recovery plans

Overcoming Objections

Disaster recovery is like insurance. Some clients might think it's just something nice to have instead of a necessity. They might have various reasons for not considering disaster recovery as a priority, such as:

- "It's too expensive."
- "It's too complicated."
- "It'll never happen to me."

The fact is that unwanted events happen all the time, regardless of the cause. Disaster Recovery planning is really no longer an option for any business because of this. According to FEMA, "40% of small to mid-sized businesses never reopen after a disaster, and an additional 25% reopen but fail within a year." Comparing the costs of a DR strategy with the potential costs incurred from an inability to maintain regular business operations can effectively garner support for your service. Comprehensive BCDR planning could be the difference between the two-thirds of businesses that don't survive and the one-third that do.

COST OF DOWNTIME BY INDUSTRY

IT	AUTOMOTIVE	MANUFACTURING	HEALTHCARE	BROKERAGE	RETAIL
$145- $450K per hour	$3M per hour	$260K per hour	$636K per hour	$6.48M per hour	$1.1M per hour

COST OF A DATA BREACH

In 2023 the average cost of a data breach globally reached an all-time high of $4.45 million. This represents a 2.3% increase from 2022 and a 15.3% rise from 2020.

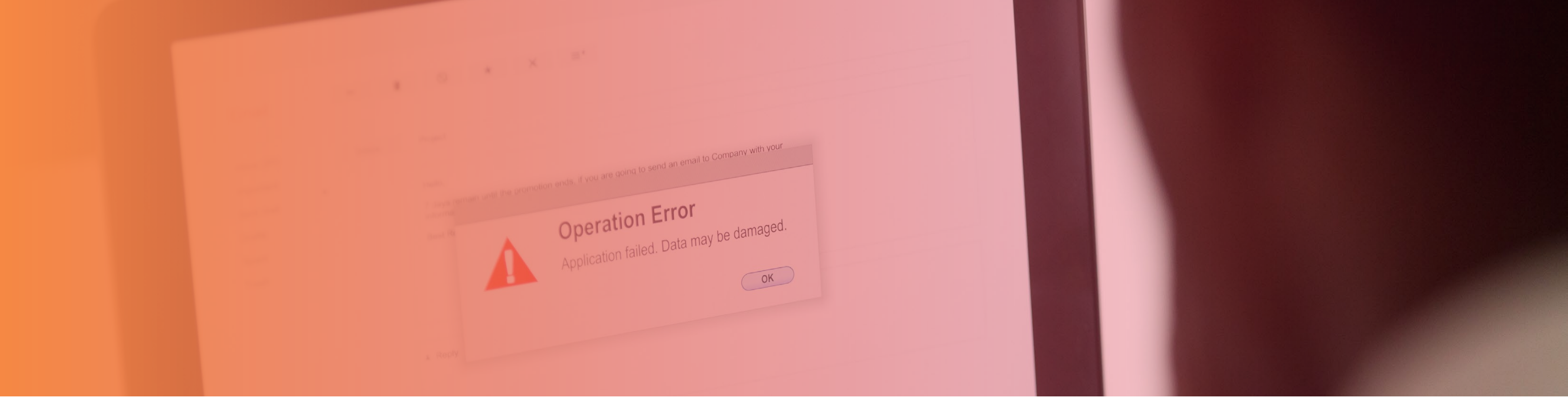
DOWNTIME AFTER A RANSOMWARE ATTACK

In 2022 the average length of interruption of a business after ransomware attacks in the United States was 24 days. This is an increase from 2020 to 2021 from an average of 15 days to 24 days for the duration of downtime.

Sources: Gartner, IDC, Atlassian, Statista, Morgan Lewis

10 Reasons Your Clients Need to Invest in Disaster Recovery

1. Minimize the impact of any disaster
2. Ensure continuous employee productivity
3. Become far more cost-effective
4. Meet compliance and regulatory requests
5. Access instant recovery
6. Reduce downtime of operations
7. Reduce potential financial losses
8. Reduce liability obligations
9. Minimize the risk of negative exposure
10. Facilitate crisis management



Operation Error

Application failed. Data may be damaged.

Downtime Causes

While a client might think that only natural disasters lead to downtime through power interruptions impacting hardware, it’s important for them to understand that software and human factors play crucial roles as well. With the technology, both internal and external threats continue to evolve.

- NATURAL DISASTERS
- PANDEMICS
- HARDWARE FAILURE AND SOFTWARE CORRUPTION
- HUMAN ERROR (WITH OR WITHOUT MALICIOUS INTENT)
- CYBERATTACKS

Calculating the Cost of Downtime

Lost Revenue + Lost Productivity + Recovery Costs + Intangible Costs = Downtime Cost

LOST REVENUE

This is fairly easy to comprehend. If your clients 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 nonrevenue related activities. Salary or hourly wages, or 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 an employee time required to recover lost data
- Physical tools/ devices that may need repair or replacement
- Cost of lost data

LOST INTANGIBLE COSTS

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

Offer Additional Managed Services With BCDR

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, Scale Computing can deliver BCDR services on your behalf. Partners are available whose expert disaster recovery services can be white-labeled.

Contact your account executive to find out how Scale Computing Services can help you with the following:

- BCDR Planning
- SC//Platform Cloud Unity
- Zero Downtime Hardware Refresh
- Zero Downtime Memory Upgrade

CONTACT US

SCALE COMPUTING

CORPORATE HEADQUARTERS
525 S. Meridian Street - 3E // Indianapolis, IN 46225
P. +1 317-856-9959 // scalecomputing.com