The MSP’s Guide to Selling Backup

How to position backup, business continuity and disaster recovery solutions for your SMB clients.

pax8.com

Why MSPs Should Value Continuity/Backup Recovery

Cybercriminals no longer need to “hack” systems; they log in using Living Off the Land (LOTL) techniques, exploiting built-in tools to launch ransomware in hours instead of weeks.[1]

With ransomware, human error and hardware failure on the rise, attacks are inevitable. What matters is how fast clients recover. By positioning continuity as essential (forget optional), you safeguard operations, build trust and unlock new profit streams as their MSP advisor.

From Human Error to Ransomware: How Backup Recovery Saves SMBs

Backup is a business necessity, not a choice. From cyberattacks to simple mistakes, continuity is the lifeline against these vulnerabilities.

User error

From accidental file deletion or overwriting to spilling coffee on laptops, user error is the primary cause of data loss.

Ransomware attacks

Even if you pay a ransom, you may not get all of your data back.

Breaches

This includes phishing, password theft, network intrusions, malware and more. Bad actors have multiple methods to gain access or corrupt valuable data.

Malicious deletion

Where employees delete critical data out of spite for termination or to cover their tracks.

Employee turnover

Well-meaning departing employees sometimes try to "clean" their devices and file systems before leaving.

Hardware failure

Hardware failures, such as device or server crashes, can lead to massive data loss.

Device loss or theft

Mobile workforces increase the risk of lost or stolen laptops and smartphones that contain corporate data.

Physical disasters and power outages

Fires, floods and power outages can destroy devices and servers, leading to data loss or corruption.

The Cost of Inaction for SMBs

Bad actors commonly exploit SMBs that believe they are too small to be targeted.

SMBs myths:

"We're too small"
60% of SMBs recognize they're the most likely target for cybercriminals, yet they underestimate their real risk.[2]

"We have antivirus"
1 in 3 SMBs are working with outdated cybersecurity technology and have experienced a cyberattack within the past year.[2]

"We don't have valuable data"
All data is valuable; bad actors pay between $10-$2500 for hacking and phishing services.[3]

Average Prices for Malicious Content on the Dark Web

Social security number	$6
Credit score	$7
Mother's maiden name	$15
Scam templates	$25
Weekly phishing kits	$170
One-time phishing kit	$1,000
Antivirus disabling	$1,000

Average Costs of Breaches and Downtime for SMBs

- A successful cyberattack could put nearly 1 in 5 SMBs out of business.[2]
- For 32% of today's small firms, losing less than $10,000 or a day of downtime would be enough to shut down business.[2]
- 55% of SMBs would go out of business with $50,000 in financial impact from a cyberattack.[2]

When selling backup, stress the urgency of lost revenue, downtime costs, losing customer trust and reputation, compliance fines and legal risks to SMBs.

How to Sell Continuity/Backup Recovery

Continuity is a form of insurance, and the cost of protection is always lower than that of a breach. The best time to sell a continuity solution is when it's sunny, not when a storm is already raging. Don't wait for a crisis to start the conversation.

Here's how to position backup as a critical business decision:

2. Lead with Stories and Statistics, Not Pitches

Real-life stories and numbers show the urgency and current business problems that affect SMBs of all sizes every day, not just in special scenarios.

Examples:

A Denver university's website, phone lines, email services and online programs were shut down during summer finals and the start of fall semester due to a malicious cyberattack.

- 54% of business workloads and apps currently run in the public cloud.[4]
- 90% of SMB respondents use native data protection tools for Azure, which they claim are unprepared for major disasters.[4]
- 60% of these data protection setups lack true disaster recovery capabilities for Azure virtual machines.[4]

2. Uncover SMB Blind Spots

Explain that data is valuable, despite the size of a business. From a customer or employee data list to credit card transactions or even accessing a public Wi-Fi space. Criminals can access your private credentials and sell them on the dark web. Focus on the key priorities of revenue, compliance and reputation.

3. Demonstrate Your Own Security Strategy

Relatability builds rapport. Clients are more likely to trust a provider that's been in their shoes. Showcase past security vulnerabilities you've corrected and allow them to see your backup strategy, increasing the likelihood of purchase and familiarity with the tools.

4. Do So Because Microsoft Says So

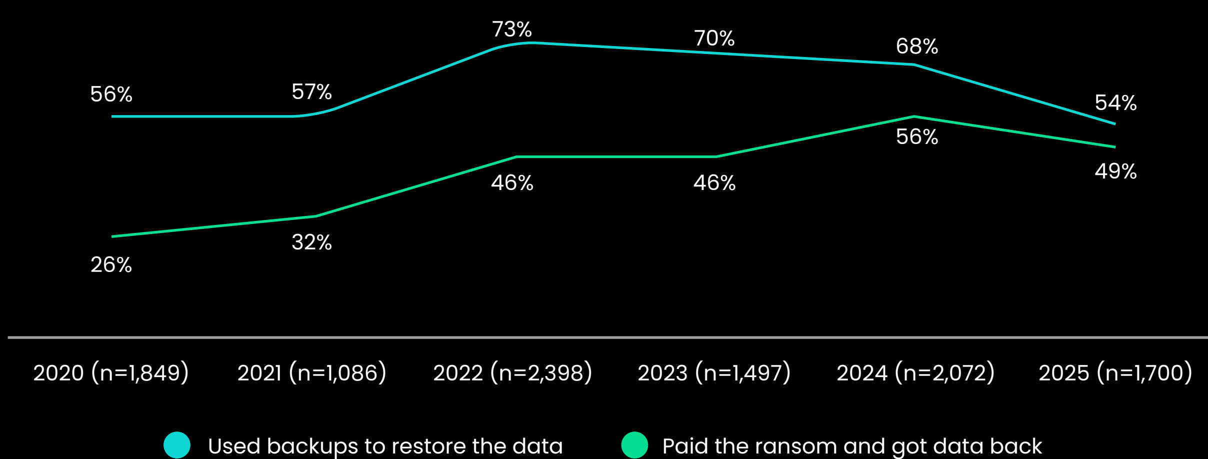
If Microsoft stresses the importance of backup and recommends third-party backup solutions, it must be true.

The Microsoft Services Agreement states:

"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve your content or data that you've stored. We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services."

About **54% of firms** restored their data using backups versus paying the ransom.[5]

Recovering Data Via Backups and Ransom Payments 2020-2025



Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart.

Source: Sophos 2025 State of Ransomware Report

The chart shows that companies with backup methods have greater success recovering their compromised data than those that paid a ransom.

5. Offer Flexible Entry Points and Build Continuity Over Time

Avoid overwhelming clients with complex BC/DR solutions or inciting fear. Start small with third-party SaaS backup and progress into more advanced solutions from there. Your clients need to start somewhere to protect their data, so getting them covered by a cloud backup solution is a great first step.

Discover the Perfect Client Backup Plan

Solution	Overview	Best for	Strengths	Limitations	Key Questions
Backup and SaaS Backup	Backs up files, folders and SaaS apps (M365, G Suite). Data stored in cloud/off-site.	SMBs, laptops, desktops, cloud apps.	Affordable, low maintenance, supports compliance, reduces risk.	Slower restores.	How much/ how often do you back up? How long does recovery take?
Business Continuity (BC)/Disaster Recovery (DR)	On-site and cloud backup appliance to minimize downtime.	Critical apps, high-risk geographies, compliance industries.	Fast recovery, reduces downtime, ransomware protection, supports compliance.	Costly, restore time varies.	Do you need to meet compliance? Experienced ransomware? Did recovery fail?
High Availability	Real-time replication of systems/ data for zero downtime.	Businesses that cannot afford downtime.	Continuous availability, strong disaster recovery, efficient replication.	Expensive, more than some SMBs need.	If you lost access to data, would you be out of business?

Combat SMB Objections

It’s natural for SMBs to hesitate, whether because of limited knowledge, tight budgets or the belief that more security isn’t necessary. Your role is to guide them. Use these responses to address concerns with clarity and build confidence when overcoming barriers to purchase.

“We’re too small to be targeted.”	Cybercriminals assume defenses are weaker with SMBs. Most cyber breaches happen to companies with fewer than 1,000 employees. Continuity ensures you can recover all your data when that happens.
“We already have antivirus and firewalls.”	Advanced attacks can easily slip past these defenses. Even with strong security, ransomware, phishing and human error still slip through. Backup and recovery are about resilience, so you can bounce back when defenses fail.
“Our data is in the cloud, so it’s safe.”	Cloud providers like Microsoft and Google don’t guarantee recovery if files are deleted, corrupted or held ransom. Continuity gives you control and restores your data when the cloud can’t.
“We don’t have anything hackers would want.”	Every business offers valuable data (customer records, financial information, employee files) that is sold on the black market. Losing access to your data hurts your ability to operate. Continuity safeguards both company operations and data.
“Downtime wouldn’t really hurt us.”	Most businesses underestimate the cost. Downtime can reach hundreds of dollars per minute once lost sales, productivity and recovery expenses add up. Continuity turns unpredictable losses into predictable investments.
“It’s too expensive.”	Continuity is a low-cost investment compared to downtime, lost clients or ransom payouts. You hope never to use your insurance, but it can save your business thousands when you need it.
“We’ll deal with it if something happens.”	Recovery without a plan is risky and impossible. Once data is lost or encrypted, it’s usually too late, creating stress and chaos. Continuity ensures your business keeps running smoothly instead of scrambling in crisis mode.

Putting It All Together

Continuity is business survival, not a luxury. SMBs need it. MSPs profit from it.

Your playbook:

- Prove the cost of downtime
- Demonstrate that ransomware is inevitable
- Position continuity as insurance
- Start small, scale big
- Future-proof with automation

With the right mix of backup, BC/DR and high availability, you safeguard clients, grow your revenue and secure your role as their trusted guide in the age of cyber overwhelm. Connect with one of Pax8's solution consultants to discuss which business continuity solutions are right for you and your customers.

Schedule a call

Sources

1. 2024 ThreatDown State of Ransomware
2. 2025 SMB Threat Landscape Viking Cloud Report
3. SOCradar 2024 Dark Web Report
4. State of Backup and Recovery 2025 Report
5. Sophos 2025 State of Ransomware Report