MSP360

MANAGE. SUPPORT. PROTECT.

REPORT

MSP360 2025 State of Managed Backup

1-866-4-MSP360
1-415-301-7773

sales@msp360.com

6425 Living Place Suite 200
Pittsburgh, PA 15206

msp360.com

About This Report

While services around data protection should be a staple for every MSP, there remain opportunities for MSPs to add, augment, extend, and fine-tune managed backup and recovery-related services based on client requirements and in the interest of remaining competitive.

And with the need for business resilience quickly becoming — if not already being — an expectation on the part of your clients, offering a comprehensive and effective managed backup can mean the difference between an MSP that ensures measurable resilience for its clients and one that merely performs backups.

To provide context to MSPs on the current state of managed backups, we surveyed 150 MSPs to shed some light on what their clients are most concerned about, what data and operational disruptions you should be prepared to address, and how your peer MSPs are taking their managed backup services to market.

Key Findings

Below are some of the key findings from this year's State of Managed Backup report:

When looking at those who ranked each of these disruptions as one of their "greatest concerns", **cyberattacks dwarfed the other disruptions by as little as 2:1 and as much as 4:1**, demonstrating its prevalence in client's minds as a viable risk to their business.

Nearly 88% of client organizations can only stay operational **less than a week** after a disruption event, with 50% of client orgs **only surviving a day**.

Two-thirds of client organizations have experienced one or more operational disruptions in the last 12 months.

87% of the disruptions experienced by an average MSP client organization last one **business day or less**.

The average MSP sticks to simple backup & recovery and leaves out the opportunities found in backing up cloud and endpoints, as well as in offering disaster recovery planning.

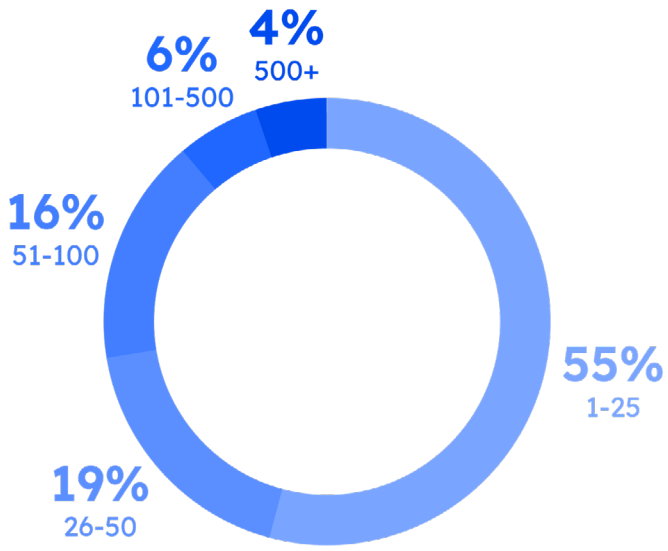
Only 4 out of 10 MSPs have backup & recovery bundled in their cybersecurity or managed cloud offerings

About the Survey

We surveyed over 150 MSP organizations throughout the globe during the month of October 2025 that specifically offer backup and recovery services of some nature to their clients.

We received the greatest number of responses from MSP organizations in the United States (47% of respondents), Europe (24%), Latin America (20%), and Asia (9%) in this year's report.

The sizes of client organizations based on employee count (shown at right) provided us with a solid representation of MSPs taking care of every size org, breaking out the smaller (and more common) org sizes, using standard breakpoints for small organizations, with representation into midsized organizations.



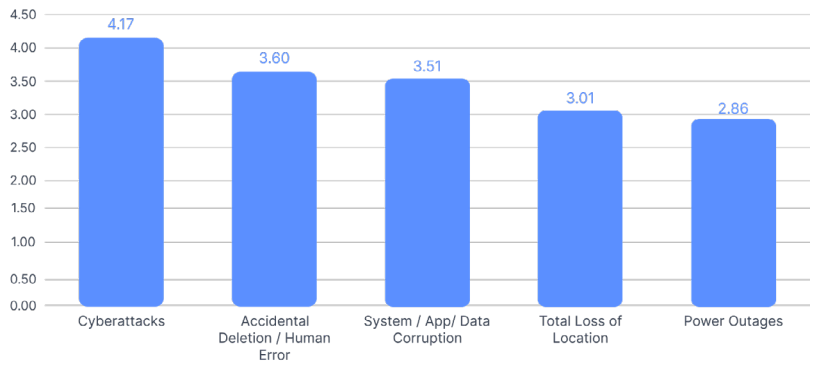
MSP360 2025 State of Managed Backup Report

Are MSP clients concerned about business disruptions?

The typical MSP client organization is usually small enough that, should they experience a disruption in operations of a material nature, they will feel the pain in a very real way. Shown below, over half of MSPs' clients can only endure a loss of operations for a day before it becomes painful. An additional 36% of MSP clients can tolerate a week's disruption.

In short, **SMB clients aren't going to handle a business disruption well, nor for very long**.

So, which disruptions are they seeing as viable risks to their business?



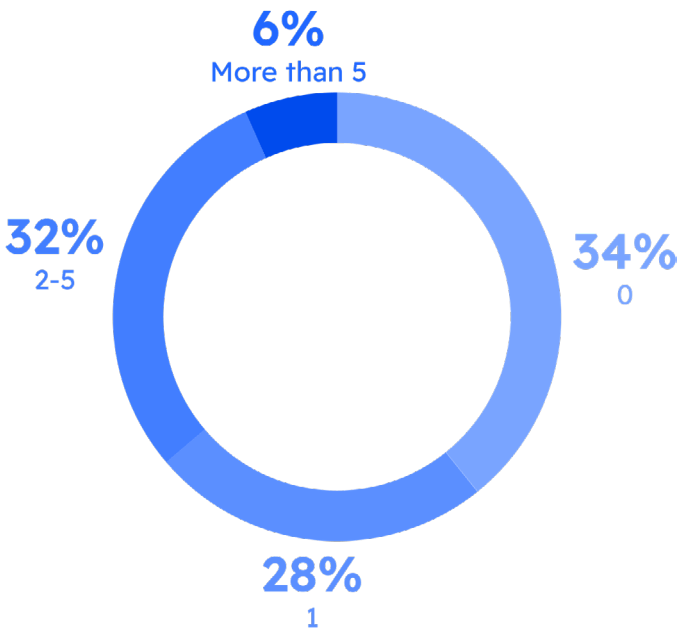
As shown above, when asked to rank how concerned MSP clients are with five very real types of disruptions on a scale of 1 to 5 (with 5 being the highest), cybersecurity ranked as the highest risk.

Given that the other disruption risks are possible but not as probable as an impending cyberattack, it's good to see that **SMBs are realizing the threat reality of cyberattacks**.

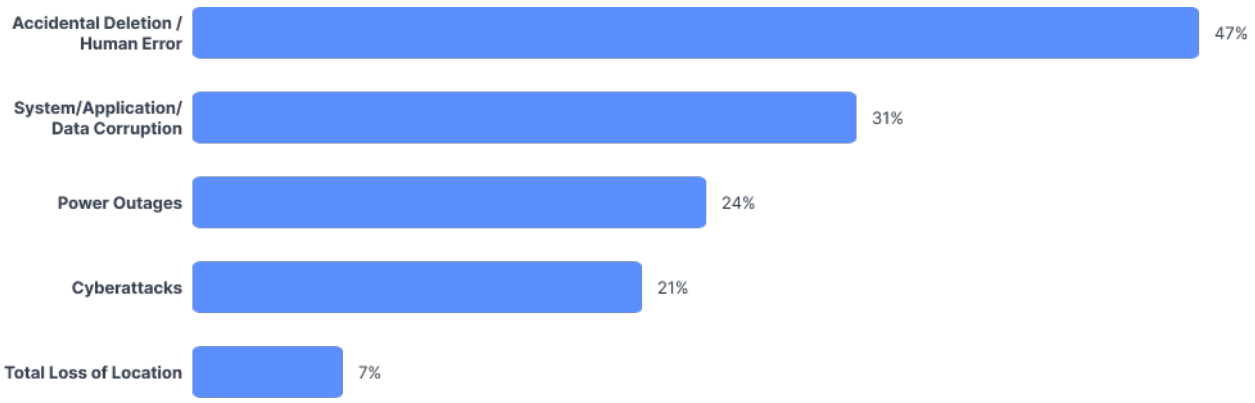
So, what's the source of the concern?

State of Business Disruptions

SMBs are both experiencing the reality of cyberattacks firsthand, as well as are simply keenly aware. As shown at right, MSPs say 66% of their SMBs clients have experienced one or more cyberattacks in the last 12 months, demonstrating that their clients' concern for cyberattacks is personal. However, just over a third (34%) of MSPs that indicated their clients have not experienced a single cyberattack—contrary to expectations—still showed concern levels consistent regardless of past incident experience. The analysis of the data shows that there is less than a 1% variance in the degree of concern for cyberattacks between those MSPs whose clients have experienced cyberattacks and those whose clients have not.



When asked what kinds of disruptions have been experienced by their clients, MSPs indicate that cyberattacks are actually one of the least occurring disruptions. Accidental Deletion of Data, System/Application/Data Corruption, and Power Outages have all been experienced by more MSP clients than Cyberattacks, with only Total Loss of Location trailing behind.



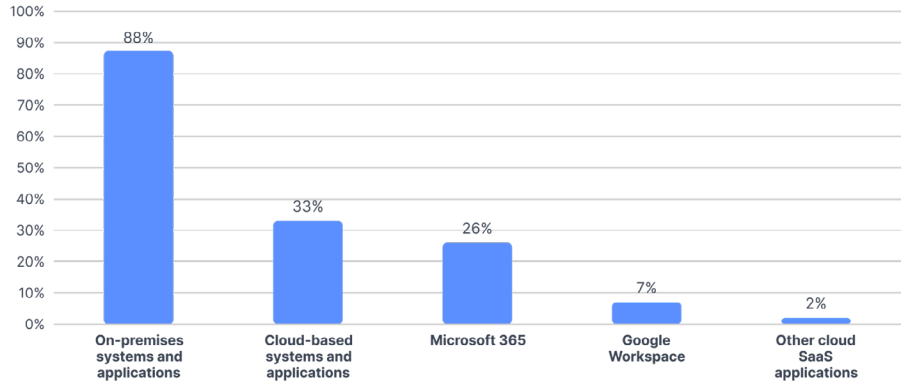
% of MSP clients experiencing specific types of disruptions

When experiencing these disruptions, MSPs estimate that 87% of their clients' operations were out for one business day or less. This is good news, but still cause for concern, because MSPs have already told us that half of their clients can only tolerate a single business day without operations before it materially impacts the business, any disruption that takes longer than a single day to recover from will have a material impact on some MSP clients.

So what data, if any, was lost?

Are MSP Clients Experiencing Data Loss?

In a word, yes. We see in this year's data that **38% of MSP clients have experienced data loss**. As shown below, the most prevalent form of data loss remains on-premises systems and applications, dwarfing any of the cloud-based applications or data.



Keep in mind that none of this means the 62% of MSP clients that "haven't" experienced data loss didn't initially lose data due to the issues previously raised, such as accidental deletion or cyberattack. Instead, it means that **despite the disruption, MSPs that have backup and recovery of their clients' data**, applications, and systems in place are able to recover the data, mitigating any permanent data loss in most cases.

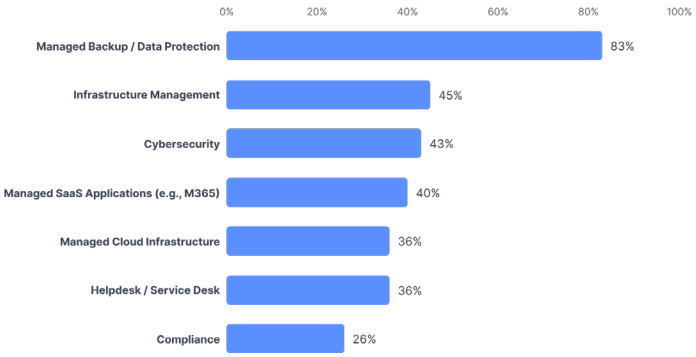
In other words, **backup and recovery are not only working but are vital parts of ensuring clients stay operational**.

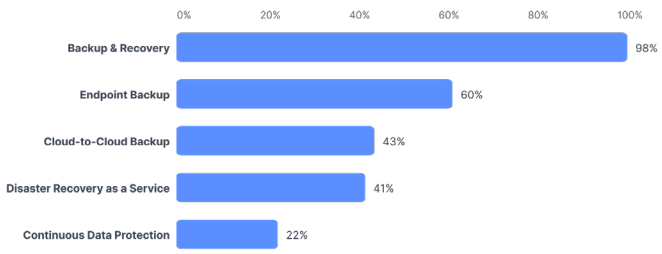
So, how are effective MSPs offering managed backups to their clients?

How is Managed Backup Being Offered?

While nearly all MSPs provide basic backup and recovery, few have expanded to advanced services that differentiate their offerings. As shown at right, backing up endpoints and cloud application data are offered by far fewer MSPs. And more mature data protection services like DRaaS and CDP are even less frequently seen.

At a minimum, MSPs today should be offering Cloud-to-Cloud backup to ensure the data residing in platforms like Microsoft 365 and Google Workspace is protected. The assumed Shared Responsibility cloud model dictates that backup of customer data in these platforms is the sole responsibility of the customer (and you, by extension). And Disaster Recovery as a Service provides MSPs with the opportunity to offer additional service components around planning for, frequently testing, and delivery of recovery should a disruption occur.





The majority of MSPs also seem to stick with a traditional “Managed Backup” service offering, shown at right. Keep in mind that the other services listed (e.g., Cybersecurity) provide MSPs with avenues to either introduce backups to a client, or augment which data sets are being backed up (and, therefore, recovered)—and yet, MSPs aren’t taking advantage of the opportunity.

The reality is that you should have backups as a cross-functional part of nearly every service (as is appropriate, of course) to ensure data protection is always top of mind with clients. Expanding beyond traditional backup not only **increases client resilience but also creates recurring revenue opportunities through premium services**.

Managed Backup Recommendations

Managed backups, in and of themselves, are a protection play; they’re designed first and foremost to provide the client with the ability to recover the systems, applications, and data they need to remain operational. But today’s client organization needs to be resilient, not just “recoverable.” This is the opportunity for MSPs: to shift the conversation from “we can restore your data” to “we can make your business resilient in the face of a disruption of any kind.”

To this end, here are a few recommendations:

Shift from Recovery to Resilience

Half of client organizations can only survive being down for a day. Another third for a week. These insights should drive client conversations about acceptable downtime, critical workloads, and continuity planning.

Integrate Backup into Cybersecurity

Less than half (43%) of MSPs have backups tied to their cybersecurity service offering. When a cyberattack strikes, you need to not only bring the client environment back to a known-working state but also a known-secure state. That is, you need to be able to recover any and all systems, directory services, etc., that were touched during an attack to ensure they are no longer in a compromised state where threat actors could regain access and/or control.

Evolve Toward DRaaS

If your service today is merely defining data sets and setting up backup jobs, you're missing out on the opportunity to offer customers a sense of comfort — knowing not just that you can pull the lost or impacted data from a backup, but actually knowing you can get their environment back up and running quickly. Shifting from a managed backup offering to DRaaS can be as simple as including a business impact analysis, a risk assessment, building out recovery plans for specific types of "disasters," and running recovery testing — whether that be a tabletop exercise or a trial recovery to a virtual cloud recovery environment. These additional functions add value to the service and work to ensure you have a plan when a disruption event hits your clients.

Include Protecting the Cloud

With 57% of MSPs not including the backing up of cloud platform data in their managed backup offering, it's evident that offering this is not only a smart choice, but one that's necessary to ensure you're protecting all of your clients' data—regardless of where it resides.

Conclusion

Throughout this report, we've seen how SMBs get affected by business disruptions, and how MSPs can help not only to meet growing client expectations but also to guarantee protection, business continuity, and operational efficiency. The data shows a clear trend: MSPs who streamline their service delivery and centralize backup management are better positioned to prevent data loss, reduce downtime, and grow profit margins.

That's where MSP360 comes in. With MSP360 Managed Backup, MSPs can reduce maintenance time and provide seamless multi-tenant management for large-scale IT environments. With centralized management, you can monitor multiple endpoints in one place and configure and track multiple backup restore jobs — all without juggling numerous solutions.

Alternatively, you can streamline your operations with the MSP360 Platform, an all-in-one suite designed to standardize your services and enhance delivery. Built on the reliable foundation of MSP360 Managed Backup, the platform also includes powerful tools for remote monitoring and management and secure remote access, helping you manage and support client environments more efficiently.

About MSP360

Established in 2011 by a group of IT professionals, MSP360™ provides simple and reliable cutting-edge Backup and IT management solutions for MSPs and IT departments worldwide.

MSP360™ platform combines the number one easy-to-use backup solution to deliver best-in-class data protection, secure remote access software to provide support to customers or team members, and painless RMM to handle all aspects of IT infrastructures, all under a single pane of glass.