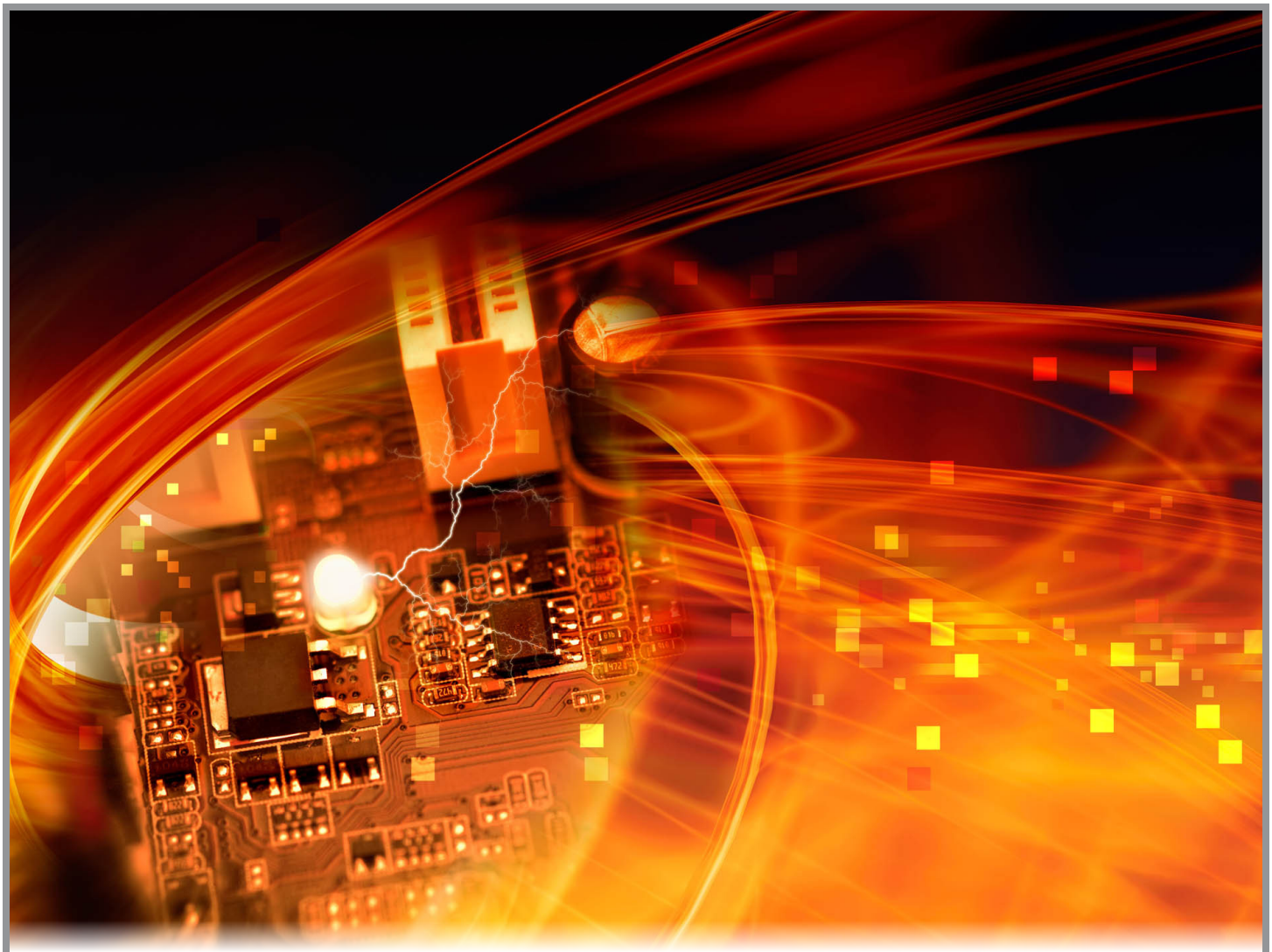
WHITE PAPER



Leaving Nothing to Chance: How Backup and Recovery Bolsters Managed Services Offerings

By Pedro Pereira

N-able

INTRODUCTION

Like it or not, data loss is a cost of doing business. Whether as a result of unintentional or malicious action, the typical business at some point loses data. Eighty percent of businesses that participated in a 2011 Ponemon Institute study revealed they had lost data within the previous 12-month period.

The question then becomes whether a business can recover lost data. While data loss seems inevitable, it doesn't have to be debilitating. With the advent of cloud computing, data backup and disaster recovery (DR) has become more accessible and affordable for companies large and small. And no one is better equipped than the MSP (managed services provider) to deliver the services as an integral part of an overall package to remotely monitor and maintain the IT environments of their clients.

The opportunity for MSPs is significant. An October 2011 Computer Technology Industry Association (CompTIA) study, "Trends in Managed Services," revealed backup and DR is not one of the top 10 managed services offered by MSPs. This indicates MSPs stand to profit handsomely by providing a high-value service to clients that pays dividends not only in revenue but also in customer satisfaction and loyalty. Here are the most compelling reasons to offer the service to clients:

- New revenue opportunities
- Competitive differentiation
- Client lock-in
- Ability to demonstrate value in catastrophic situations

MULTIPLE DATA THREATS

In 1859 a massive solar flare that turned the night skies over North America and Europe different shades of red, green and purple, disrupted telegraph communications around the world. The "Carrington Event" sent billions of tons of solar plasma onto the atmosphere, igniting paper in telegraph machines and lighting sparks on telegraph pylons.

Imagine a similar occurrence in the digital age. Such an event would potentially disrupt the electrical grid and the Internet, causing convulsions in computer networks around the world. A severe electromagnetic storm could cause massive data losses and overall damages of up to $3 trillion. But you don't need to imagine a catastrophic solar event to understand the causes and effects of data loss. Hurricanes, floods, earthquakes—all of which affected the U.S. Eastern Seaboard in a two-week period in 2011—can cause property destruction and power failures, forever erasing important data.

Further darkening this picture, consider data losses caused by malicious activity. A succession of attacks on corporate networks has caused data losses in a spectrum of organizations, including credit card, payroll processing and retail companies, the U.S. Congress, the CIA, and even the Sony Playstation Network. In 2007, it was revealed the FBI had lost 160 laptops over 44 months. Companies also lose data by accident—inadvertent file deletions, unsecured file sharing, and failure to back up systems. According to a recent CompTIA study, most losses occur when data is in motion, including unencrypted email, Internet downloads and uploads, use of USB flash drives and unsecured WiFi connections.

Be they a result of malicious activity, inadvertent action or nature's fury, data losses are costly and, in some cases, fatal to a company. For companies still using tape backups, the average cost of downtime is at least $145,000 and recovery takes up to 20 hours. Of companies that suffer a major data loss, 43 percent never reopen, 51 percent close within two years, and only 6 percent survive long-term.

RISK-TAKING CULTURE

With so many potential threats to data, IT administrators could be forgiven for giving in to paranoia. Yet, a culture of risk seems to pervade the small and midsize (SMB) business space where the necessity to prepare for disasters with data backup and DR strategies is not fully understood. This is especially the case with the smallest businesses, where the prevailing attitude appears to be, "It won't happen to me."

A recent study by security vendor Symantec uncovered that 50 percent of SMBs had experienced financial, legal and personnel issues as a result of failing to properly store and back up data. The study found 25 percent of SMBs don't back up at all, and 50 percent store backup files in the same location as their computers without off-site replication. According to industry estimates, companies that use data backup and DR solutions, whether large or small, typically spend only 2 percent to 4 percent of their overall IT budgets on the technology.

The cost and physical space requirements of legacy storage and backup systems to some extent explain the risk-taking culture among SMBs. But even larger companies have experienced a fair share of problems with backup and recovery. Tape remains the dominant backup and DR technology, and as it has been demonstrated time and again, the technology is unreliable. The research firm Gartner has concluded recovery from tapes works only 40 percent of the time. Tapes are easy to damage, sometimes get lost in transport, and often malfunction unnoticed during the backup process.

REGULATION COMPLIANCE

Organizations that lack clearly defined business continuity strategies and data backup processes, or shrug them off altogether, are taking a significant risk. Aside from potentially putting themselves out of business as a result of an unrecoverable loss, they could run afoul of federal and state regulations that impose severe fines for preventable data losses.

Federal laws such as the Sarbanes-Oxley (SOX) Act of 2002, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Federal Information Security Management Act

(FISMA) of 2002, and Canada' Data Protection Regulations have placed strict security, storage and recovery requirements in place for companies handling sensitive data such as finance, medical and legal records.

Regulations cover just about every aspect of data handling, including data creation, electronic transactions, email and data transport, as well as archiving and recovery. Any organization that creates, transmits and receives the data has to be able to demonstrate compliance.

Compliance can be daunting, especially for companies in the SMB space, who are affected not only by the federal regulations but also those of the states in which they operate. For them, the surest way to ensure compliance is to retain the services of an IT trusted advisor who can help end clients wade through the morass of legislation, devise a data protection, storage and recovery strategy, and implement the strategy for the client.

MANAGED SERVICES ADVANTAGE

No one is better positioned than the MSP to help businesses safeguard and archive their data, and to have it ready for fast recovery when necessary. Cloud-based, remotely managed backup and DR solutions are tailor-made for MSPs, who for the better part of a decade have been leveraging remote monitoring and management (RMM) tools to prevent downtime and improve performance in their clients' IT environments.

It is not hyperbole to affirm that RMM transformed the IT services channel. Before RMM, service providers were reactive, often seeing clients only when troubleshooting was needed. The future of an IT services business was largely uncertain because of a disproportionate revenue reliance on the next big sale or the next client project.

RMM changed all that by making possible the automation of IT services delivery and, with it, the generation of predictable monthly or quarterly revenues for service providers. From their own or co-hosted datacenters, providers now can remotely spot trouble before it happens. For instance, they can prevent a mail or file server from overloading or identify potential network traffic logjams that would affect user productivity and, ultimately, profitability.

In providing managed services, MSPs have achieved a level of insight into their clients' environments that they could only imagine before RMM. The technology not only allows them to proactively manage their clients' networks, but also puts them in a position to act strategically to better prepare clients for future business and IT demands.

As such, the addition of cloud-based backup and disaster recovery to managed services offerings is an ideal fit for MSPs that differentiates them from the competition while creating a new revenue opportunity. With a small increase in the monthly customer fees, MSPs have an opportunity to significantly increase their value to clients, many of which cannot afford expensive tape or disk-based on-premise recovery systems. It is a logical extension of the RMM services MSPs already deliver.

From the client's standpoint, the appeal of managed services is the ability to prevent problems by monitoring servers, applications and the infrastructure, which vastly reduces the need for costly troubleshooting of IT environments. Managed services, however, cannot completely prevent the possibility of downtime because they cannot forestall events such as natural disasters, earthquakes, fires or terrorist attacks. And that means managed services without a business continuity component effectively leaves a crack in the dam that at some point could have disastrous consequences. Backup and DR, therefore, should be an integral component of any MSPs' business strategy.

REMOTE BACKUP

While RMM prevents downtime, backup and DR solutions minimize downtime and accelerate recovery. DR lets organizations resume applications, data, hardware, communications and overall IT infrastructure. N-able Technologies, a global provider of RMM automation software for MSPs, provides partners with an easy, affordable way to deliver high-availability remote data backup and DR to their clients. N-able offers Backup Manager, based on CA Technologies' ArcServe D2D R16 backup technology, as an add-on to the N-able's N-central RMM platform.

Backup Manager is a scalable, centrally managed disk-based solution that reduces backup and recovery costs while accelerating restore times. For MSPs, the add-on technology creates an opportunity to add value for clients to meet Service Level Agreement-stipulated recovery times while adding to the RMM revenue stream.

Without budget-busting upfront investments or burdensome maintenance requirements for clients, MSPs have an opportunity with Backup Manager to protect their clients' servers, desktops and laptops through a pay-as-you-grow model that allows clients to add capacity as needed. It's easier to add a few dollars to existing managed services fees than to ask for a large upfront payment.

Backup Manager delivers multiple replication options—one-to-one, many-to-one and one-to-many. MSPs can back up multiple servers to a local backup server on site by installing software agents on the backup server and on the machines that are being backed up. A full backup image of the software is created at the compression level for each server from which individual files can be restored as needed.

Block-level incremental backups copy only the data that has changed since the last backup, using less storage space and accelerating restores. Single-snapshot backups leverage five restore types to move only data that has changed and rapidly restores files, volumes, individual emails and entire databases to any previous backup point in time.

Backup Manager features also include:

Virtual server protection: A single-user interface helps protect virtual and physical servers, simplifying operations and reducing training times. Migrations from physical to virtual servers, or between two virtual servers, allow for flexibility and easy management.

Bare metal recovery: Crashed servers are recovered very quickly to the same or dissimilar hardware, reducing to minutes a process that can take up to 36 hours.

Encryption: Whether data is stored on- or off-site, or a combination of both, it is kept out of sight of unauthorized eyes.

Backup throttling: Customized backup performance processes balance system usage, keeping mission-critical applications performing while protecting data.

Centralized management and reporting from N-central: While helping to prevent expensive data loss, centralization reduces expenses and ensures protection consistency.

Integration with cloud-based storage: Off-site replication, remote archiving and additional storage capacity is delivered with the flexibility and scalability of the cloud.

SIMPLIFIED PROCESS

RMM vendors typically offer monitoring capabilities for existing backup solutions, but N-able took a different tack through deep-level API integration with CA Technologies' best-in-class ArcServe technology. In the process, N-able made backup and DR an MSP-ready solution by simplifying scheduling, reporting, management and deployment activities. As such, MSPs have a "single pane of glass" to manage the whole process, which eliminates the need for multiple consoles that often bog down technicians and administrators.

By embedding data backup and DR in the RMM platform, N-able gives MSPs all the technology they need to easily manage client environments from a single source. From a practical standpoint, this is a significant business benefit of simplifying billing and reducing the burden of invoices.

CONCLUSION

In its "Managed Services Trends" study, CompTIA found that 19 percent of end-user organizations outsource backup and DR to a provider, while 44 percent prefer to keep it in-house and 36 percent use a mix of both. Since backup and DR is not one of the top 10 services offered by MSPs, it is safe to conclude the opportunity for them to add backup and DR is significant. MSPs, therefore, must make backup and DR an integral part of their offerings to offer a truly comprehensive set of services to monitor, manage and protect their clients' IT environments. ■

N-able