Cashing in on the Next Wave in Backup and Storage

Here's what experts consider table stakes for backup and storage today, and how MSPs can help customers make the right choices and increase recurring revenue at the same time. **By Karen D. Schwartz**

Credit: iStock / miakievy

A **FEW YEARS AGO,** a small business hit with ransomware experienced something all companies dread—an attack that targeted its backups. At first, the company didn't think much of it, assuming that its data was protected. The company's small IT staff started the recovery process, reloading all the tapes, and then went home to get a few hours of rest.

But they miscalculated the tenacity and ingenuity of today's hackers. In fact, the perpetrators were still in the system during the tape reloading process. Through malware they had previously installed, the bad actors were able to delete the contents of all of the tapes, largely because the IT staff was so exhausted they had missed flipping the "write protect" tab on the tapes. As a result, the situation went from what could have been a recoverable event to one where the company was forced to pay the ransom.

All this happened during the time the company was in contract negotiations with Alvaka Networks, an Irvine, Calif.-based MSP specializing in backup, disaster recovery, and ransomware recovery. In fact, this incident sealed the dealt for the company, and its executives immediately signed the paperwork for all three services.

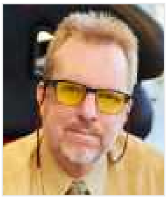
What happened to this small business isn't uncommon. As many as 88% of SMBs experienced at least one ransomware attack in the last year, making them much more vulnerable than larger enterprises. What's more, 46% of ransomware victims that paid the ransom were attacked again. But that's only part of the problem; many small businesses can't survive for long if they are attacked. In fact, less than half of SMBs would survive for three days after an attack, and 28% would survive for only seven days.

Today, backups are prime targets for bad actors who have created increasingly sophisticated methods of attacking the backup administration console and changing backup jobs or retention policies. After getting inside, it's just a matter of finding and deleting directories or inserting a virus into a backup. When a company attempts to restore its environment from a backup, it unintentionally restores the virus into its production environment, which causes it to detonate. As a result, companies end up either losing weeks or months of data or paying a ransom.

It doesn't help that organizations often don't have effective backup technology or processes, says Oli Thordarson, CEO of Alvaka Networks. For example, it's not uncommon for companies to use the same credential for managing backups as they do for managing the rest of the IT infrastructure—definitely not a best practice.

As a result, many businesses need to rethink their backup practices, but because data storage and backup are intrinsically linked, those practices also affect storage. While data backup focuses on keeping data secure, that data resides in some type of data storage repository. That's a large part of the reason why storage vendors also have begun adding ransomware detection into their storage systems and including workflows that use storage snapshots to recover from ransomware before it gets to the point of backup.

> "SMBs might be too small of a target for some attacks, but on the other hand, they are more likely to be selected randomly and hit by a bot—and bots don't discriminate."



OLI THORDARSON
CEO, Alvaka Networks

Chad Kempt, CEO and owner of Fast Computers, a Canadian service-based MSP, recalls a company that became a customer after experiencing what he referred to as a horrible situation.

"They were storing their data on a NAS [network-attached storage] device and didn't have any backups other than some PCs with USB backups of select data," Kempt explains. "When disaster hit, their data was encrypted across the entire network extremely quickly, taking down their entire business, line-of-business applications, and important documents. They had to try to quickly figure out where their data was, restore it, and reinstall their programs to get business operating again."

Since then, the company has become a client of Fast Computers and moved forward with a security plan to protect endpoints.

These types of issues create a lot of opportunities for MSPs to assess the environment, pinpoint the biggest weaknesses, and address them with modern backup/recovery and storage systems and processes.

The biggest tool MSPs have in their arsenal is knowledge. For example, while many SMBs believe they are too small to be a ransomware target, it's up to MSPs to dispel that myth.

"SMBs might be too small of a target for some attacks, but on the other hand, they are more likely to be selected randomly and hit by a bot—and bots don't discriminate," Thordarson says.

Modern Backup Makes a Difference

Largely as a result of ransomware, modern backup and recovery tools have changed and matured. Simply put, older backup technology isn't robust enough or effective enough anymore. Here is what experts consider table stakes for backup today:

IT MUST BE IMMUTABLE. Immutability means that files can't be changed in any way during a set retention time, which can either be a specific period of time or forever. "You can't just copy the data and put it in another location," explains Brent Ellis, a senior analyst at Forrester Research. "To deal with issues like ransomware and other cyberthreats, it's critical that the data can't be changed, or hackers could compromise the credentials, delete the backups, and then re-encrypt the data." Ellis recommends using write once, read many (WORM)-based storage, which enables the data to be read as often as needed, either via tape or cloud-based object storage, or a hardened storage array.

Yet while immutability is table stakes, it's not fully embraced by SMBs. One study found that 21% of SMBs have no offline immutable backups, creating an opportunity for MSPs to fill that gap.

AIR GAPPING IS ESSENTIAL. A physical air gap disconnects the backup from the network after it is written and then reconnects the network, while a logical air gap sends backups to a physically separate location but they aren't completely disconnected from the network. The backup software prevents the backups from being overwritten or deleted.

The need for air gapping and protecting against ransomware means that the 3-2-1 backup rule (having three copies of your data, with two of the backups stored on different types of media and at least one backup stored off-site or in the cloud) isn't good enough anymore, says Greg Schulz, founder and senior advisor of StorageIO, based in Stillwater, Minn. Today, he says, there should actually be four versions with at least three copies in at least two different places, one of which is offline and another in the cloud, all at different points in time. Without the emphasis on different points in time, it's much more likely that all three copies could be corrupted, he explains.

Either way, air gapping works. "We've done recovery with clients that do have good backups, and that's usually because they had some sort of adequate air gapping," Thordarson says. "That makes their issues much less severe; they typically don't have to pay the ransom, they usually get all of their data back, and they can recover more quickly, usually with less drama."

FIX BAD PRACTICES. While ineffective backups often occur because older backup systems can't handle modern threats effectively, sometimes it's just a case of bad practices building up over time, says Raj Goel, owner of Brainlink International, a New York-based MSP.

"The most common problem we run into is that prospective clients have backup software, but when you actually look at it you see that they are either backing up data they no longer need, aren't backing up critical systems that have been replaced since the last time they did a refresh, or that the backups aren't working at all," he says.

As an example, Goel describes a customer that was backing up a server that hadn't been used in five years, but at the same time, the company's actual production data wasn't being backed up.

Improving Storage Hygiene

By far, storage capacity is the biggest storage problem companies encounter today, partly as a result of the way they now use data, partly because of unprecedented data growth, and partly because of poor data hygiene.

> "To deal with issues like ransomware and other cyberthreats, it's critical that the data can't be changed, or hackers could compromise the credentials, delete the backups, and then re-encrypt the data."

BRENT ELLIS
Senior Analyst, Forrester Research

Companies are expected to create data at a rate of 1.4 million gigabytes per second by 2024, and while small businesses won't reach that level, they are still on target for massive data growth. This results in a situation where companies are constantly running out of storage. While it's tempting to simply buy more, MSPs can sometimes help by improving storage hygiene—essentially going through data stores and deleting what's no longer needed. And sometimes, it's just a matter of reducing data sprawl.

"Over time, businesses often end up with data in several different places," Goel says. "We've run into situations where clients have their data in Google Drive, Dropbox, OneDrive, and Evernote, and a third-party SaaS tool and a NAS on-site."

In addition to making it very difficult to inventory data, this scenario can result in duplicate file and folder names. Sorting this out is painful, but it's a necessary step in improving a company's storage situation.

Adding additional storage can incur unexpected costs for small businesses, especially in the cloud. For example, companies that rely on cloud services and need to increase the amount of storage can end up paying more than expected. In other cases, a company that needs to move data between one cloud service and another can be hit with hefty storage egress fees; in addition to the per-gigabyte storage fee they already paid, they must pay per gigabyte when reclaiming the data.

Another ways MSPs can help small businesses is by ensuring that storage is immutable for backup purposes. Not only does this protect data against malware, but it helps avoid accidental file deletion or modification, improves compliance and data authenticity, speeds up recovery times when disaster strikes, and protects backups against retention policy changes and deletion of restore points. At the same time, immutability must be adjustable, and production data isn't a good candidate for immutability because users will probably want to modify it at some point.

Finally, today's storage must be performant. "There is no sense in having super-reliable immutable storage if customers can't get their work done because of unacceptable performance," Kempt observes. "That's where the cloud dilemma arises. If you're on a bad rural internet connection dealing with large CAD files, you're going to run into performance problems."

The Cloud Conundrum

Deciding whether to recommend that customers rely on the cloud or on-premise-based backup and storage, or a combination of the two, is one of the most important factors in optimizing those solutions.

It's about what is appropriate for the com-

Credit: iStock / miakievy

pany and the workload, Kempt says.

"If the customer has a lot of data on-site and a poor internet connection, or only one connection with no redundancy, it makes sense to keep data on-premise. But if they are primarily using applications in the cloud, we often push them into pure cloud because there is no benefit anymore to keeping things on-premise," he says.

Kempt describes one customer that had switched from a traditional office environment before the pandemic to a work-from-home setup where users needed access to all data at all times. As a result, Kempt's company switched the customer to Office 365, migrated its main application into Azure, and moved the file storage into SharePoint and OneDrive. All data is now shared through Teams. For another customer that works on very large files with high-performance demands, he implemented all-flash storage in an on-premise server with 10G to every desktop.

GREG SCHULZ

CHAD KEMPT

Opportunities for MSPs

Of course, an assessment is crucial. While the "bits and bytes" conversation is important, Goel says that most of the discussion is actually nontechnical.

"It's about where the business is today, where it will be in five years, and what it needs to get there," he says. "I've been telling my customers for years that they pay a 30% tax that doesn't show up on their financial statements. It's a productivity tax because Becky can't find an email or Bob can't find a drawing or Jane can't find a contract."

Sometimes, it can be difficult to convince small businesses that they need to upgrade or replace their existing backup and/or storage. Yet, there is plenty of opportunity to win these companies as clients, according to a CompTIA survey; more than half of small businesses currently use MSPs for some portion of tech support, and an additional 36% are considering it, according to one survey. And the SMB Group found that SMBs that accelerated tech adoption during the pandemic were more likely to experience increased revenues than their peers—a good selling point.

These technologies, bundled with the right services, can be very profitable for MSPs. For example, a backup-based service should yield MSPs at least a 70% gross margin, and it could be as much as 85%, Thordarson says.

"It comes down to the services you bundle with it," Kempt says. "If you're just reselling a service, that's one thing, but if you're bundling your managed services around it and actively monitoring and testing it over time, profits rise."

Making the right choices for your customers while making the most profit also requires carefully vetting the vendors you partner with, Goel adds.

READER ROI

- **RANSOMWARE**, along with capacity and efficiency issues, make this a great time to help customers upgrade their backup and storage.
- **DONE RIGHT**, MSPs' services can improve their customers' backup and storage while reaping significant profits from recurring revenue.
- **WHILE THE TECHNOLOGY** is important, effective processes are also critical.

"The last time ransomware hit one of our clients was in 2005, and it was expensive, painful, and embarrassing," he recalls. "But we learned from that. We learned that some of our vendors hadn't been honest with us, so now the only way we will partner with a vendor is by investing a lot into proofs of concept and testing."

KAREN D. SCHWARTZ *has written hundreds of feature articles, hard news pieces, white papers, case studies, and book chapters on a variety of technology and business topics. She resides in Potomac, Md., and can be reached at karen@karendschwartz.com*