

Step-by-step guide: data protection.

By Alan Radding

When the topic of data protection comes up for discussion with IT leaders, a company's size is irrelevant. "Mid-size organizations have the same need to protect their data as big enterprises, only they have fewer resources to do it," says Mike Karp, principal analyst at Ptak, Noel & Associates. For any business, if the data is compromised or inaccessible for any reason, the organization soon comes to a halt. "It's a question of how long you can function without access to your data," he continues.



The answer: only a few hours, Karp suggests. A day or longer without access to its key data raises questions of whether the business can survive. In addition, depending on the industry, an organization may fall under regulations mandating protection of certain data.

"Data protection means backing up data, usually to tape and now disk," notes Greg Schulz, senior analyst, StorageIO. Mid-size organizations, however, face challenges when it comes to data backup. It has traditionally involved a complicated process, often requiring specialized IT skills and extra costs. The virtualization of servers, a growing practice, also complicates data protection, as do government mandates to safeguard the privacy of particular data.

Industry analysts generally agree on a six-step process for protecting data. Mid-size organizations may not follow all the steps, but at least they should know what to do and what their options are.

Need data protection products?

Dell's data protection and recovery products for the mid-market.

Disk Based Products

Removable disk backup & continuous data protection solutions.

dell.com.sg/business/disk-back-up

Tape Based Products

Reliable backup solutions for large amounts of data and long-term archiving.

dell.com.sg/business/tape-back-up

Step 1

Assess, inventory, and classify your data

This is a matter of identifying all data, where it is located, and how it is being protected today. Then managers need to classify it in terms of its importance to the business. Some data, like transaction data or customer data, will be critical. Other data less so.

Finally, check to determine which, if any, of the data falls under a regulatory mandate. If you are storing confidential personal information, such as social security numbers, it can require special protection.

Step 2

Determine RPO and RTO

The key metrics when it comes to data protection are recovery point objective (RPO) and recovery time objective (RTO). These metrics are integrally tied to how much a business needs to invest to achieve sufficient data protection.

> **RPO** is the point from the past, whether two hours or two days, to which you aim to recover your data.

> **RTO** is the time you will accept to restore your data in the event you need to recover it.

The general rule of thumb: The closer the RPO and RTO get to zero, the more it costs. Mid-size organizations usually can get by with an RPO and RTO of hours or even a day. If so, they can greatly reduce the cost of data protection without incurring significant business risk. This is why it is important to classify the data at the outset. Not all data has the same value or needs the same RPO and RTO.

Step 3

Understand the data protection options

There are an increasing number of options for data protection. Industry analysts generally identify three primary options for mid-size organizations. These are: back up to

tape; back up to disk, often in the form of a virtual tape library (VTL); and remote replication.

> **Tape backup** is the data protection mainstay for mid-size organizations. Backup software tools know how to handle it; the process is well understood, even though somewhat cumbersome and slow; and tapes can be moved off-site for greater protection.

> **Back up to disk**—the emergence of low-cost disk drives makes it possible to back up data to disk. Disk allows for faster and more reliable data backup and recovery. After a time, typically a week to a month, organizations often will move the backed up data to tape to free up disk space for more backups. VTL makes the disk appear as tape to the backup software so organizations need not change their backup process.

> **Remote replication**—sends copies of the stored data over the network to a remote site where it can be stored on disk or tape. This provides an added measure of protection.

"Think of remote replication as a hedge against disaster," says Karp. Moving tape off-site provides a similar hedge.

Step 4

Choose the right combination of options

"No one option is right for every mid-size business, and many organizations use multiple options," says Schulz. Data that needs the lowest RPO and RTO can go to disk-based backup or VTL while backing up less frequently needed data to tape. It comes down to assessing the criticality of the data and understanding the RPO and RTO trade-offs.

In some cases, companies might replicate data to satellite offices for safety, but it should be backed up first. "Satellite offices almost always lack the resources to protect

the data," says Karp. If the objective simply is to get the data off-site, you also can ship tapes to the remote office for safekeeping.

Step 5

Address the virtualization challenge

The advent of virtualized servers complicates data protection. "In a virtual server environment a sound data protection strategy is particularly important," says Schulz. Unfortunately, some virtualization products currently "lack tools for complete data protection," he notes.

The basic virtualization backup tools allow the backing up of the entire virtual machine (VM). Recovering data requires restoring the entire VM first. However, usually companies want to restore only a file or two, not everything. Vendors are introducing proxy products to address this need.

Step 6

Encryption and compliance

Depending on the industry, there are mandates to protect the privacy of certain data through the use of encryption. This is particularly true when data is being sent over a network.

In the event of any kind of data breach, many regions have laws requiring personally identifiable data be encrypted. Otherwise, if there is a data loss, companies must inform everyone whose data might be compromised. To avoid that possibility, many companies choose to encrypt stored private data.

Today mid-size companies have numerous data protection options at very attractive prices. In addition, vendors have been adding intelligence to the products to simplify the process. With easy, low-cost tape and disk backup options available, there is no reason to neglect protecting data.

Alan Radding is an experienced freelance business and IT analyst/writer based in Newton, Massachusetts.