Business continuity and disaster recovery

A business risk advisor should help evaluate how much data loss can be absorbed in case of a failure

May 10, 2018 Joerg Laves

A dental office in the Lakes Region is the latest example of how natural disasters can undermine your business continuity.

During a recent storm, the dental office experienced repeat power outages when the power lines were struck by lightning. Even though the office's system had surge protectors, the server failed overnight, requiring the IT vendor to call the next morning for a same-day power supply replacement. Despite the warranty promise, the server manufacturer could not locate and install a spare immediately, causing more than two full days of lost business.

Keeping business running when disaster hits

In the broadest sense, Business Continuity and Disaster Recovery (BCDR) is a strategy that allows a business to function no matter what. While everyone likes to talk about hurricanes, fire, flood and Nor'easters, a more common need to rely on BCDR technology is much more mundane: accidental data deletion, virus and malware, theft of equipment, mischievous activities by disgruntled employees and hardware failure.

Any backup is better than no backup, but occasionally backing data files up to a USB drive is not sufficient in most cases. Which method to choose depends on how long a company can function without access to their data.

Let's use the dentist office as an example, using the issue of computer server failure.

Most dentists heavily rely on access to their data, and, in most cases, must shut down the practice if they cannot access patient records. If the office has three dental hygienists generating revenues of $175 per hour, and two doctors generating $800 of revenue per hour each, a day without access to their patient information system creates a revenue shortfall of $17,000 for each day they are down. And there are additional hidden costs, such as the risk of losing patients when treatments must be rescheduled for another day.

Assessing risk

When designing a business continuity solution, your business risk advisor should help you evaluate how much data loss can be absorbed in case of a failure. If data is not easily reconstructed, you will need very short backup intervals. This is referred to as the recovery point objective (RPO). In a transaction-dominated environment, the RPO should be as small as possible to minimize cost of a failure.

You should also look at how long a recovery can take without significantly impacting your business. This is the recovery time objective (RTO). The longer the recovery takes, the higher the impact on the business.

To illustrate these concepts, consider the dentist office. Suppose that the practice backs up data files directly to the cloud every night at 6:00 pm. One day, the server crashes at 4:30 pm and must be rebuilt. The recovery point is over 22 hours ago, so all transactions entered since the last backup the day before at 6:00pm are lost and have to be reentered.

To restore the server that requires rebuilding, the practice's IT technicians must feed disks to the server and recreate all user information and install all programs. Then, IT needs to download the data files from the cloud backup, which, depending on the size of the data files, can take hours. Restoring a server from scratch can easily take two days or more. In this instance, the RPO is 22.5 hours, and the RTO is 2 to 3 days. For most businesses, this delay would affect staff morale and customer interactions, and certainly the bottom line.

Selecting a better solution

Using a smart business continuation strategy, the dental practice's outage could look very different. Support can be provided so that all data files are backed up to a BCDR device in 5-minute intervals. If the company's server fails, the monitoring software could alert the technical staff to immediately virtualize the server on the BCDR device. This can be done from a mobile device within seconds of the failure. Without delay, the BCDR continues to act as the server until the failed server can be repaired or replaced. This process is performed without disrupting the staff's data access and user experience.

When the server is finally ready, the BCDR device initiates a "bare-metal-restore" to automatically transfer control to the rebuilt server without any user interruption. In this case, the RPO is five minutes and the RTO is zero, a significant improvement over the first scenario in this article.

Joerg Laves is managing consultant and owner of IT Secure in Manchester. He can be reached *at jlaves@itsecureservices.com.*