

# Automating the Backup Process

## Value

Explosive increases in the quantity of data in digital format (i.e., email, faxes, application data, documents, and media files) is fueling small businesses and large enterprises to need data storage and backup technology like no other time in the history of the electronic age. Despite a sharp increase in affordability and availability of automated backup systems, many businesses still rely on unsecure tape devices to backup and restore vital information.

Further, management may not fully appreciate the risk they take by neglecting backups in favor of "more important" issues. Any non-expert can observe that data loss frequently occurs even with a backup system in place. According to a 2004 Enterprise Storage Group survey, nearly one in four SMBs reported that at least 20 percent of their recovery attempts fail.<sup>1</sup> Cited as the primary cause for data loss: human error—in the backup process, or in the interchange and handling of tapes.

Automation is the "automatically controlled operation of an apparatus, process, or system by mechanical or electronic devices that take the place of human labor."<sup>2</sup> Automation is widely understood to be beneficial but perhaps misunderstood to be costly or difficult to implement or both.

## The Story

The following article, written for a Home Care Automation Report about healthcare providers, illustrates the practical, real-world differences in the operational requirements and impacts between traditional removable media backup solutions like tape, and newer automated local and offsite backup solutions.<sup>3</sup>

### Scenario 1:

*"Your network application and file servers are backed up to a standard tape drive every night. In the mornings, it is your job to remove one or many tapes from their drive(s) and examine log files to make sure the previous night's backup(s) completed without errors. When that is done, you transport the tapes to an off-site location or prepare them for pickup by a courier service. When the courier swaps your fresh tapes for another set of tapes from your offsite rotation system on the same trip, you insert them into the proper drives, either immediately or at quitting time.*

*You have previously checked into the safety and security of the offsite tape storage service, which replaced your pre-HIPAA offsite storage site: your bedroom dresser drawer. The courier and offsite storage facility are well worth their monthly fee, considering the peace of mind that accompanies knowing your data is housed in a fireproof building behind a hefty lock.*

*Once a month, or perhaps quarterly, depending on the policy specified in your company's disaster recovery manual, you perform a practice restore from tape to disk to validate your backups. The practice also serves to refresh your own memory of the steps involved to perform a restore so that you can do it efficiently should the need arise to do it under the pressure of an emergency. This does not have to be a complete restore, as data on tapes can be presumed valid if just a few files restore properly. However, it must be done in such a way that it does not overwrite new files with older ones of the same name. This means your periodic test restore must be done between the time overnight backups finish and the first person comes to work the next morning.*

*Once a year or so, you purchase new tapes to replace existing ones before they wear out and become less reliable. Once or twice a year, you train someone else to perform this daily routine so you can go on vacation."*

### Scenario 2:

*"You contract with an online, offsite backup service and pay their monthly fee. Your network connects to the service's network through a broadband connection. Backups initiate automatically, either nightly or several times per day, depending on choices you have set up via a web-based application. Your data is encrypted and transmitted to two redundant, secure locations in two different parts of the country, on servers behind bank-vault-like doors that can only be opened with handprint recognition.*

RELEASE 1

AUGUST 2009

<sup>1</sup>"The Changing Dynamics of Backup and Recovery in the Small and Medium Business (SMB) Market," John McKnight, The Enterprise Storage Group, June 2004.

<sup>2</sup>"automation" Merriam-Webster Online Dictionary. 2009. Merriam-Webster Online. 25 June 2009 <<http://www.merriam-webster.com/dictionary/automation>>

<sup>3</sup>"Disaster Planning: Online, Offsite and Out of Sight, Could the Internet Be the Future of Data Backup?" by Tim Rowan originally appeared in *Home Care Automation Report* ([www.homecareautomationreport.com](http://www.homecareautomationreport.com)) February 7, 2007. Reprinted with permission.

*When a minor emergency occurs, such as an accidentally deleted file, you go online, locate the most recent version of the file and restore it through the same broadband connection. When a moderate emergency occurs, such as a server crash, you replace the hardware and operating system and then re-image the new hard drive(s) from the remote backup servers, again using a web application. When a fire, hurricane or earthquake hits and it may be days or weeks before your servers are replaced and your building is inhabitable, your patient data can be accessed through the Internet as soon as you can get to a working, connected computer."*

## Keep it on Schedule

When an end user deletes a file that they did not intend to delete, or when a disaster strikes, natural or otherwise, there should be no concern regarding whether data will be retrievable.

The Barracuda Backup Service is configured to run backups on a schedule. The first time data is backed up, all of the files are pulled from servers on the local network. The files are examined to ensure they are unique, they are broken into parts, tagged, compressed, encrypted, and then transferred offsite using an existing Internet connection. In subsequent backups, the server identifies new or changed files, keeps a local copy and then sends a copy to the offsite data center. This process happens automatically every time a backup runs.

Once data is transferred offsite and confirmed by Barracuda Central, it is automatically replicated to a second secure data center using Barracuda Networks' bandwidth and resources. When a customer needs to restore information, their data is available from the local Barracuda Backup Server and from either of the offsite locations.

The ability to schedule backups provides multiple benefits. Employees do not have to hand-hold the backup process. IT professionals do not need to monitor each server being backed up and switch the tapes in and out. No one needs to take the tapes offsite at the end of the night for data security in case of a disaster. No one needs to exchange tapes with a data vaulting service.

Automatically scheduled backups are guaranteed to happen every day. They do not take sick days, get too busy with escalated technical support requests, or accidentally overwrite yesterday's tape with today's data, and they won't go home without backing up your servers.

Because the process is automated and because the schedule can run as frequently as necessary, a benefit is created that tape backup cannot replicate – version availability. For a business with critical data that changes frequently throughout the day, a more aggressive backup schedule is warranted. For example, instead of once per night, the schedule can be set to look for changes every hour. Perhaps an employee deleted a paragraph from a word file they were working on in the morning and would like to have it back. Restoring the file is as simple as pulling up the Web interface and finding the applicable revision.

## Assurance

Firmware updates and security patches are automatically delivered to the Barracuda Backup Service through updates included with the offsite subscription plan. When a scheduled backup completes, the Barracuda Backup Service reports successes and failures. The system administrator receives an email with a list of all new, changed, or deleted files included in the backup. The Barracuda Backup Service also generates warnings for inaccessible shares, folders, or files. If the local Barracuda Backup Server is offline or cannot communicate with Barracuda Central, the administrator is going to know. Through the Web Interface, administrators have access to a number of statistics and graphs that display everything from processor load to bandwidth utilization to the efficiency gained by compression and deduplication technology.

## Recovery is the Goal

Ultimately, the goal of the Barracuda Backup Service is to have quick, easy, and uninterrupted access to critical data. Even in a less critical data loss scenario, consider how long it takes to locate and load the correct tape to retrieve a file. Now consider a disaster scenario and how long it would take to recover gigabytes or terabytes of data across multiple (dozens or even hundreds) tapes. An automated offsite solution keeps stress levels down by keeping the recovery process as simple as possible.

*For questions about the Barracuda Backup Service, please visit <http://www.barracuda.com/backup> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.*



**Barracuda Networks**  
3175 S. Winchester Boulevard  
Campbell, CA 95008  
United States  
+1 408.342.5400  
[www.barracuda.com](http://www.barracuda.com)  
[info@barracuda.com](mailto:info@barracuda.com)