Data backups: The basics

Most organizations diligently perform daily backups of their data and assume that the data will always be available. Few are thoroughly prepared for an incident such as an office fire or flooding. Although backups are in no way glamorous (just ask any IT person how much they enjoy managing the backup process), they can be the lifeline for organizations when disaster strikes.

Keep them safe!

Backups such as DTL tapes, DVD's or other media must be protected with the utmost care. It is unfortunate too see that many organizations do not appreciate the risks present when backup media is simply stored on the desk of a systems administrator or in a wall unit in full view of employees and visitors. Backup media contains highly confidential data whose disclosure could have a wide ranging impact. Sometimes the risk of not storing the backups appropriately is even greater than the benefit of having backups in the first place. When considering backup solutions and storage, management should always have in mind the possible consequences of having their confidential data lost or stolen. All backup media should be stored in a secure location which is locked, equipped with security devices and environmental protection such as fire suppression and proper air conditioning.

Send them offsite

All too often, I see organizations not storing their backup media at an offsite facility for economic reasons. The results of such decisions can be devastating. Fires and the ensuing flood from fire suppression, theft or sabotage are all risks which warrant that every organization which deals with critical data such as personal and financial information should have backups stored periodically at offsite locations. A setup which is frequently seen in the Cayman Islands is to have an employee take the backup media home at the end of each business day. Although it makes sense at first, it is an incident waiting to happen! For one, the employee may forget the backup media in the car, making it vulnerable to theft and to destruction by the heat inside the parked car. Secondly, once at the employee's home, the media is subject to all kinds of risks such as children playing with the media or the employee accessing or copying data he is not allowed to see. In fact, having backup media stored at an employee's house in many cases is less secure than only storing the backup media in a locked office onsite. Furthermore, the designated employee may be absent or on vacation; will anyone else think to take the media home those days? The employee may have a very busy day and simply forget to take it; will someone notice and take it home with them that evening?

Make sure you rotate

Once an offsite backup schedule is in place, an adequate rotation schedule must be defined. The rotation of media can be defined as a method for backing up data where multiple media (such as tapes or DVD's) are used in the backup process. The media rotation schedule determines how and when each media is used for a backup job and how long it is retained once it has backup data stored on it. For example, many organizations will be comfortable with having one week of data

plus a media containing data from the previous month-end and the previous year-end. That way, if any data is missing for the last week or even the last year, chances are they will be able to restore it.

Test your backups periodically

The testing of backup media is probably one of the most overlooked tasks in the entire backup process. Organizations need to make sure that their backups are working properly and that they can be used when needed. If backups are not periodically tested, organizations may be in for a surprise when they try to restore lost data. In an incident a colleague of mine witnessed, an organization, unbeknownst to them, stored their backup media near a magnetic source. Everyday, they made their backups diligently and rotated them appropriately. No one ever noticed that the backup media was being rendered useless once stored near the magnetic source. Had the backups been tested periodically, the IT operators would have noticed the problem and corrected it before the backup media was needed in an emergency situation.

Discard your media properly

Backup media all have an expected lifespan. After a certain amount of use, it is prudent to replace backup media according to the manufacturer's specifications. After multiple uses, the risk of failure, especially from tape based media, grows significantly. Organizations must pay special attention to how the used backup media are discarded, even though the data was deleted. The best solution is to physically destroy the media, rendering it unusable and making data impossible to recover. For organizations with highly confidential data, this should be the only option. For data which is not as confidential, backup media could be reused for less-critical functions (remember, these are heavily used tapes) but data should be properly purged before. There are numerous commercial applications which will delete the data safely and make sure that it cannot be recovered even with specialized forensics software.

The bottom line for data backups is to do it regularly, securely store the media onsite and offsite and to test their efficiency periodically.