Communicating With Sam

It's Backed Up But is it Secure?

Sam Johnston

Question:

We have read recent reports of backup tapes in transit to off-site storage facilities that have been lost or fallen into public hands. Our management is concerned that this could happen to our iSeries backup tapes. What methods are available to ensure that our information is secure even if our backup tapes were to fall into the wrong hands?

Answer:

Recent highly publicized incidents have made this a serious issue and a valid concern for many organizations like yours. Today most companies have off-site storage for backup tapes as part of their disaster recovery plan and this puts sensitive corporate data and, in some cases, personal information in the hands of personnel outside of your direct control. There are many millions of pickups and deliveries of backup tapes every year in North America. Most providers of off-site tape storage services have very high service levels however even if they are 99.999% accurate this means statistically that 10 pickups or deliveries out of a million go missing.

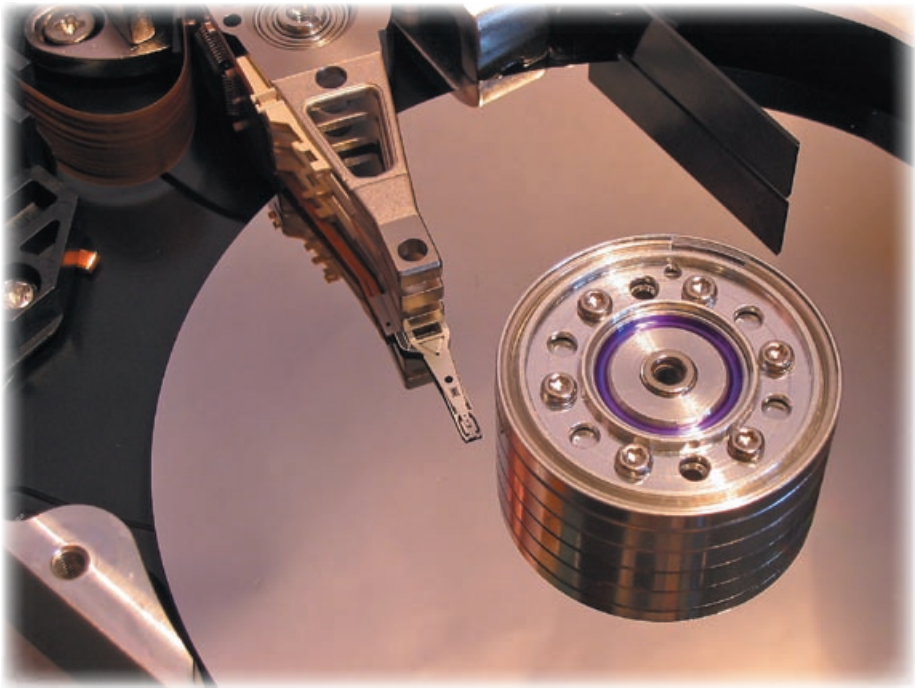
The issue is that anyone with the right authority, another iSeries and the right tape drive can restore that information and have access to it or copy it without your knowledge. The fact is that commonly used recovery practices have not addressed the increased requirements to protect personal information, and sensitive corporate data from an inadvertent breach of privacy.

The best method to ensure your information stays private is to encrypt all backup tapes and any tapes you create for exchange with business partners. This means your backup processes and disaster recovery processes will change to reflect the encryption method you choose.

The three most popular encryption methods are 3DES, PGP, and AES. These methods offer a high degree of security and are commonly used in industry today for communication purposes. To apply these methods to the back up process it's worth looking at some non-IBM hardware or software solutions.

The 3DES method is best-accomplished using hardware. There are two choices here. The first is to buy a tape drive that has hardware encryption capabilities. The SafeTape products are the most well known for this purpose. They also offer a hardware device that can be used inline on SCSI and fibre channel interfaces between the iSeries and your existing tape drive. Both of these solutions offer transparency to OS/400 generic commands, in house scripts, and backup solutions like BRMS and others. This offers effective encryption for tapes sent off site, between corporate sites and secures tapes within a shared library.

PGP stands for "Pretty Good Privacy" and contrary to its name it is a standard for strong encryption and data security. The public/private key encryption technology that is a part of PGP is recognized world wide as the strongest data security software available. The best implementation on the iSeries is the software appli-



Disk drive photo by Vladimir Markovic (http://sxc.hu)

cation Alliance PGP. It is an option for Alliance FTP Manager, which can fully automate the sending, and receiving of encrypted files as well as backup files on tape. Since Open PGP is very common on other platforms this is an effective solution for cross platform support and information exchange with partners.

The Alliance PGP solution provides a full implementation of PGP encryption, decryption, signing, and key management functions on the AS400 and iSeries platform. There is no need for a separate PC or UNIX server for encryption services. Alliance PGP fully supports Additional Decryption Keys (ADK). ADK is a critical component to support data recovery and regulatory compliance rules. PGP implementations that support ADK provide a means of recovering data you send to your trading partners, and provide an auditable proof of the data content. PGP implementations that are based on Open PGP do not support ADK, and don't provide this level assurance.

AES (Advanced Encryption Standard) has been adopted by many U.S. government agencies. It's one of the approved methods for the payment card industry, and meets the privacy requirements of medical industry regulations. This method is best implemented on the iSeries in software using Alliance AES /400. AES offers better performance when implemented in software compared to other methods. The application can encrypt saved files of any size and the resulting files can be saved to tape. For business recovery purposes the Alliance AES is restored to a backup system to allow the keys to be used for the restore. Alliance AES has the capability to encrypt individual fields in a DB2 database so that the encryption of sensitive information like credit card numbers, social insurance numbers can be integrated into your application. The AES product has all key management functions required for creating and storing AES keys and pass phrases in a secure manner. They key store is also encrypted and backed up when new keys are created.

All of the three methods discussed will provide very good security and protect the data on your backup tapes if they fall into wrong hands. This doesn't mean they will stand up to a brute force attack where every possible key combination is tried. Generally speaking the longer the key length the more combinations an attacker will need to try, and the longer it will take to break the code. The days of leaving the front open and unencrypted backup tapes are over. These encryption methods are reasonable precautions and well proven. Your tapes should never leave home without using one of them. In fact, they should never leave the tape drive without this level of protection, even if they are going to say on-site. Remember, while the breaches that get the publicity are the ones that happen in public, most IT security breaches are still committed by internal rogue employees. Good security practices always begin at home. TUG

Sam Johnston *is a partner and Chief Technology Officer of Intesys Network Communications Ltd., providing value-added networking and e-commerce solutions to the iSeries community. He can be reached at (416) 438-0002 or via e-mail at sjohnston@intesys-ncl.com.* *Any TUG member wishing to submit a question to Sam can forward their typewritten material to the TUG office, or to Intesys. The deadline for our next issue is Friday August 19, 2005.*