

WHITEPAPER

Best Practices for Choosing and Implementing a Storage Encryption Solution



Executive Summary

Over the last few years, hundreds of corporations have been featured in headlines for data security breaches. According to the Privacy Rights Clearinghouse, the records of over 158 million U.S. residents have been exposed by security breaches since January 2005. That's more than half of the U.S. population.

Lost or stolen backup tapes contributed to a large number of these breaches, yet protecting backup data is still often overlooked. Many companies believe that it is useless to protect these tapes because they contain "old" information only used for disaster recovery (DR), but even just one compromised backup tape can cost a company its reputation, its competitive advantage, and thousands in fines. The Ponemon Institute research firm reported that data breaches cost companies an average of \$197 per compromised record in legal fees and other expenses.

Recent lost or stolen backup tapes include:

January 2008 – The Internal Revenue Service (IRS) and Kansas City officials are searching for lost agency computer tapes that may have been missing for as long as two months.

January 2008 – A backup tape containing in-store credit card information on 650,000 retail customers is missing. GE Money USA, which manages in-store credit programs for many U.S. retailers, first realized that the tape was missing from an Iron Mountain Inc. storage facility in October.

December 2007 – Data tapes containing Social Security numbers, phone numbers and addresses for up to 800 current and former employees of the state Dormitory Authority are missing. Backup tapes are sent offsite, but a recent shipment envelope was found damaged and open and the tapes were not inside.

Full list available at www.theq3.com/headlines.php

Companies are now beginning to realize the importance of protecting all sensitive customer data. The only real way to protect your backups is through encryption. This article outlines why you need to protect your stored data and what you need to look for when considering a backup encryption solution.

It's important to understand that the purpose of backup/archive encryption is to protect confidential data when it leaves the secure environment of the business on either backup tape or optical disc. Therefore, backup/archive encryption represents very different requirements from those of other internal security products designed for the network.

BOSaNOVA, Inc.

Phone: 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

Basics

Backup tapes are produced for one reason: to allow you to easily restore your data within your service-level timeframes if the original is lost or corrupted. It is imperative that you take this into consideration when looking at any proposed solution. In a real DR crisis, any complexity or additional steps required when restoring your data must be minimized. Financial institutions especially know the seriousness of restoring data in a timely fashion. In a crisis, your primary objective is to get the business back in operation; complexity must be reduced. Backups are useless if they cannot be restored immediately, from anywhere, when disaster strikes.

Once you decide that a solution is required in order to meet regulatory or good business governance requirements, a new set of questions must be addressed.

It may be that your company has a single platform environment, which could simplify the available options. Or you may be looking for a corporate-wide solution to cover a diverse heterogeneous environment. Whatever your environment, it is vital that you look at the full picture to avoid expensive and time-consuming mistakes. It is usually better to standardize on one solution for all platforms to save on training, support, and costs.

Once these questions have been addressed and the requirements understood, you must determine whether a software-only solution meets the requirement or the hardware route is the only acceptable solution. For details of the core differences between a software and hardware solution, see the table on the following page. On the hardware front, there is a choice of where that hardware should reside and this is also covered below.

The cost of a data breach

A recent Ponemon Institute survey of 9,000 people found that 12% of respondents had been notified of a data breach or loss by a company with which they did business. Of those affected, 20% said they immediately stopped doing business with the companies that couldn't keep their data secure. Can you afford to lost 20% of your customers?

Best Practices for Choosing and Implementing an Encryption Solution

	Software	Hardware
Compression	Software often does not offer compression. The maximum speed achievable will be the native transfer rate of the drive as the drive will not be able to compress the encrypted data.	Hardware units—whether built into the drive or of an inline design—use hardware compression prior to encryption, so the effective transfer rates are maintained or, in some cases, improved upon.
Speed	Software compression relies upon the system processing power to do the work; this means the speed is dependent on the available system power and is affected by other processes running on the system.	Hardware compression is not system-reliant, and the transfer rates and backup times are able to be calculated.
Upgrades	Software normally involves several updates during the life of the system.	Hardware does not change even if the complete system or OS is changed.
Encryption Availability	Software encryption is not available for all systems.	Hardware encryption works on all system types.
Configuration	Some backup packages do not include encryption and therefore require a change of package and the associated configuration as well as setup and training time to learn the new packages	Hardware encryption works on all backup packages without the need for any configuration changes.
Encryption Keys	With software encryption, the user key is kept on the system, so the system or network is open to attack.	With hardware tape encryption, the key can be kept in the device and so cannot be read from any external device.
Operating System	Software is normally restricted to a single operating system type.	Hardware is system-independent, so the same hardware can be used across many different platforms and operating system.
OS Upgrades	Software encryption usually needs to be upgraded (i.e., purchased again) when the OS is upgraded.	Hardware, being platform-independent, does not need to be changed (i.e., no cost!).
Costs	Software is often low cost.	Hardware is normally the same cost whatever the OS, so it may appear expensive on small systems and less so on larger ones.
Library	Software costs are often based on the capacity of the attached library; if the library is upgraded, you often need to pay again for the software upgrade.	Hardware costs are fixed, whatever the size of the library or the amount of data to be protected.

BOSaNOVA, Inc.

Phone: 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

What to Encrypt

Another issue that is often raised is whether to encrypt only the sensitive data (i.e., that which is covered by the various legislation) or to encrypt everything.

At first view, the concept of encrypting only the sensitive data appears to be very attractive and may offer a number of advantages. If you use a software solution, this method mitigates some of the downsides because it minimizes the amount of extra processing required by the system, and restoring the non-encrypted data is simpler. The downside is that someone has to make the decision as to what is sensitive and, more importantly, what is not. This of course is often very much a moving target. It is simple to understand that the company database needs to be secured when written to tape, but what about all those word processing and Excel spreadsheets? Ask the CEO of a major bank if copies of his/her emails are sensitive just after they have been uploaded to the Web, and you can be sure that the CEO would have preferred that they had been kept confidential. If you are going to invest in a solution, why restrict it to only part of your information?

Another area of contention is when to implement a solution. Should you look at what is readily available and “field proven” or wait for the availability of the “ultimate solution” that the vendor assures you is going to be available “real soon”? If you are in the lucky position of having a representative development system where you can run exhaustive tests of the new solution as soon as it becomes available, waiting may be an option, but what about the risk you are running until it is implemented on the live systems?

From the beginning, it should be understood that although someone in the corporate entity has identified the requirement for encryption, there may be individuals within the business who will not understand the risks and will fight against any attempts to integrate a solution into the infrastructure. Why is this?

Many MIS departments see backup and archive as a non-productive activity that simply causes them extra work and headaches. Asking them to add what they see as an additional level of complexity into this environment will not go down well. They must meet existing SLAs and will not accept anything that could potentially increase their workload and impede their primary activity of delivering a service to customers.

Another potential issue is where the funding for such a project will come from. In businesses where the financing of such projects is centralized, this is not an issue;

Best Practices for Choosing and Implementing an Encryption Solution

however, if the IT department is expected to use funds from its existing budget for something the financial department wants, you can expect some resistance.

Sometimes the resistance is because the IT group didn't get asked to evaluate a product or solution but was simply told by corporate that this is what they will be implementing. This is seen as a reflection on the professional expertise and again can add unexpected complications.

Existing Tapes

A vital point to consider is what to do with the existing pool of tapes used for backups and archives. It is likely that the rationale behind encrypting backup tapes will require that tapes written prior to the implementation of the encryption solution also be encrypted. How can this task be carried out? What extra facilities will be required? Do you have staff available to carry out what might be a considerably time-consuming operation?

If the plan is to move to a new device such as the LTO-4, is it possible to reuse the existing media, or do you have to copy old tapes onto new media and then destroy the old media? If the plan is to use new media, is there a budget to cover this additional cost, or has it been overlooked?

We are all aware that staff costs for storage management exceed the costs of the actual storage, so any new solution must not add extra work and costs for the staff managing the systems. A simple solution that requires no changes to the existing procedures or infrastructure and has no training costs in time or money may be less costly in the long term than an apparently cheaper solution that requires continual monitoring and operational input.

Are you thinking of delaying implementing a solution simply because the present system is going to be replaced in the next 12 to 18 months? By carefully selecting a solution that can be migrated to the new system, you can ensure you are safe for the whole period, not just when the new system is delivered.

IBM has announced its intention to deliver a number of security features in i5/OS V6R1 when it delivers in 2008, but can you wait until then to cover your identified security weakness? The solution that you implement on your present OS level can still be fully used when V6R1 is released. An external hardware solution with dedicated compression and encryption engines will not suffer from the problems and complexities that software such as those in V6R1 may suffer from. It also can

BOSaNOVA, Inc.

Phone: 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

be the case that the original marketing statements are simply what is intended; what is actually delivered may not have all the expected features!

The DR Implications

It is often overlooked that one of the main reasons you run regular backups is to ensure that you are able to bring up the systems required to keep the company in business in a major disaster situation. Any good tape encryption solution must be such that it does not hinder or overcomplicate this already stressful operation.

We all presume that it will never happen to us, but it does! It might be a hurricane, a flood, a fire, or an earthquake, but the result is the same: You need to restore your business data onto a new system in order to get your business back up and trading. Statistics show that if you fail to do this in a timely manner, the result 80 percent of the time is the total collapse of your business.

Be cautious against choosing a solution that's over-complex, needs specialists to install on the DR site, or has a difficult key-management system. All of these will hinder the restore process and seriously impact your company's ability to survive a disaster.

Where Should a Hardware Solution Reside?

There are three approaches to where a hardware solution can sit: in the server, on the drive, or in the layer between the two.

Hardware Built into the Server

When encryption is built into the server, it is very system-dependant and, by the nature of the beast, will be very disruptive to install. Normally, this type of encryption is designed and manufactured by system vendors, so it will have the benefits of their support and maintenance packages and may be guaranteed to be compatible with future OS upgrades.

According to the Identity Theft Resource Center, in 2007 there were over 446 security breaches affecting nearly 120 million individuals.

Lost or stolen backup tapes contributed to a large number of these breaches.

Best Practices for Choosing and Implementing an Encryption Solution

The downside of using a server-based solution is that it must also reside in any DR or development systems in order to be utilized for DR or development. This is likely to add a significant financial impact to such a project, and the disruptive nature of installing such a solution can cause substantial headaches. It also should be understood that some of these solutions use the system processors to do some of the work, so they can have an impact on overall system performance when being used.

With host-based encryption using a standard encryption card, any user who has decided to implement the same methodology will have exactly the same physical hardware as you.

Built into the Drive

At this time, there are only a limited number of truly integrated drive-based solutions on the market, and these are new and, so far, unproven. Most solutions are limited to a new media type in order to allow encryption, although they do read earlier media types and in some cases can also write unencrypted data to these media types.

All of these drives store the key externally and require external methods of controlling the encryption. The whole system's security is based on that single key as the drives are standard; hence, key management of such a product is of paramount importance.

Again, as with host-based encryption using a standard encryption card, any user who has decided to implement the same methodology will have exactly the same physical hardware as you.

Inline Appliance

These devices are normally the simplest to install and cause the least disruption as there should be no changes to the operating system and no new drivers to add because the drive type is unchanged, and the keys can be securely loaded into the appliance, which needs no network connection to the system so is inherently more secure. These systems are transparent, so they can be used on different system types and drives and can be rolled out across a heterogeneous environment very easily. If a move to another system is needed, there is no need to decrypt the data before it can be moved as the same appliance will be used to read the data on the new system that was used to write it on the original one. These solutions also offer the easiest use in a DR situation and are ideal for use when the DR site is a shared facility because their very short installation time allows them to be added only when needed.

BOSaNOVA, Inc.

Phone: 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

What's Stopping You from Encrypting NOW?

Historically, data backup is a task fraught with procrastination. Many believe that the process is complex, time consuming and costly, incurring unacceptable downtime and slowing of networks. VPN, firewalls and other security measures are widely implemented to protect data, however these are not nearly effective enough to provide the security that guarantees the safety of stored confidential records. In times past, corporations were concerned only with disaster scenarios; what if something happened to their on-site backup tapes? The answer was to transport backup tapes off-site for protection. However, as corporations grew increasingly computer and Internet savvy, the risk of employee theft, data lost or stolen during transport, environmental damage and theft of discarded tapes grew. Each of these threats brought increased security measures.

No corporation is immune to the risks involved in failing to encrypt backup data, not even companies responsible for storing the very data we strive to protect. A story released in April 2005 revealed that records storage leader Iron Mountain had fallen victim to the loss of tapes containing sensitive customer information. Because of this incident, Iron Mountain said in its statement, "Iron Mountain is advising its customers that current, commonly used disaster recovery processes do not address increased requirements for protecting personal information from inadvertent disclosure." They further went on to advise, "Iron Mountain, therefore, is recommending that companies encrypt backup tapes containing personal information..." and ended by saying, "We believe encryption is the best way for businesses to meet the increasing need for privacy protection."

Different but Better

In conclusion, all companies need to be concerned with the protection of their customer's data. It's clear that this new area of security has different requirements and issues compared with network security products and solutions, but with good planning and understanding, this solution need not be difficult to implement.

BOSaNOVA offers two storage security solutions for financial institutions looking to protect their data at rest. The Q³ is a stand-alone storage encryption appliance that's easy to use and has little effect of current backup procedures. The Q³i is a tape drive with built-in PCI compliant encryption. For more details, visit www.theq3.com or contact BOSaNOVA at 866-865-5250 or email info@theq3.com.

BOSaNOVA, Inc.

Phone: 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com