White Paper

New Demands and Requirements for Tape Encryption

How Spectra Logic BlueScale Encryption Meets User Requirements

By:

Jon Oltsik
Enterprise Strategy Group

January 2006

Table of Contents

List of Figures

The Enterprise Strategy Group, Inc.
20 Asylum Street, Milford, MA 01757 • 508-482-0188 • www.enterprisestrategygroup.com / info@enterprisestrategygroup.com

Executive Summary

In spite of a series of embarrassing "tape loss" headlines in 2005, most companies continue to turn their backs on backup encryption. Why? Most storage professionals still think that backup encryption will lead to new costs, performance problems, and recovery headaches so they continue to turn a blind eye toward the problem.

ESG believes things are about to change to radically upset the backup encryption status quo. This white paper concludes:

- **Backup encryption will move from the storage fringes into the mainstream**. Over the next few years, a combination of new privacy regulations, security threats and technology offerings will inspire large organizations to embrace backup encryption.
- **Users must learn that backup encryption goes beyond scrambling data**. As encryption becomes more routine, firms must look past cryptographic operations and consider things like key management, ease-of-use, role-based access control, and key protection.
- **Spectra Logic's BlueScale Encryption solution is in the right place at the right time.** Spectra Logic's recent entry into backup encryption is worth noting. The company has done a good job of matching security protection with management requirements and existing backup operations.

Backup Encryption Continues To Lag

The year 2005 will certainly be remembered for the number of publicly-disclosed security breaches related to lost backup tapes. In February, the Bank of America reported that it had lost a box of tapes in transit containing account information on 1.2 million federal employee credit cards. Financial services giant Citicorp suffered the same fate in June, losing tapes holding the personal information of 3.9 million customers. As the year 2005 winds to an end, Marriott Vacation Club International added another record to the lost tape annals. The travel and leisure company announced that it had lost tapes containing 206,000 employee, time-share, and customer records.

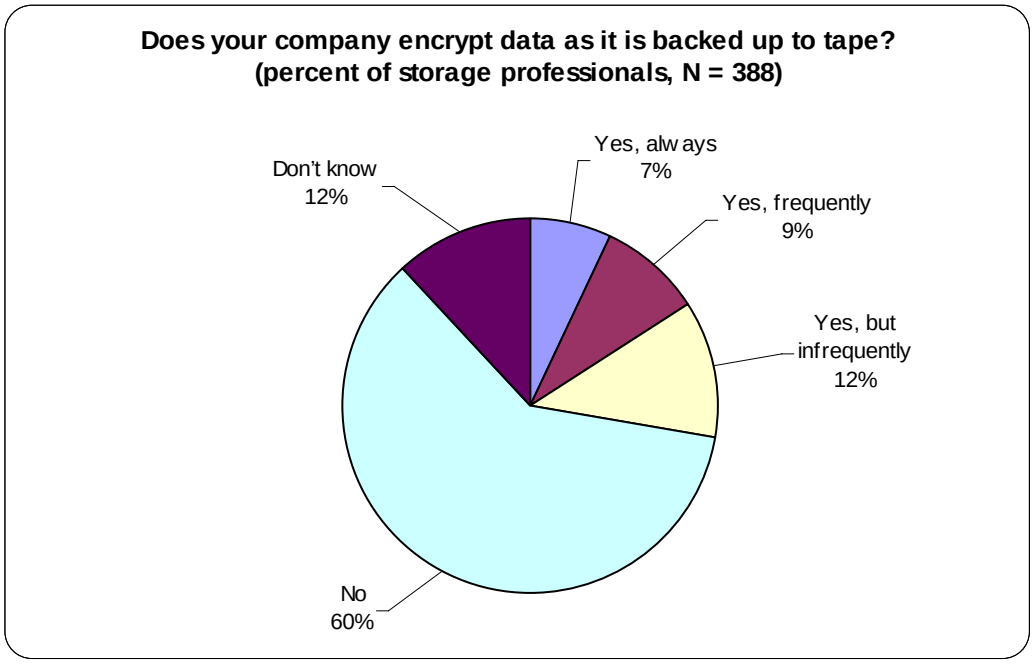
This is just a small sample of the widespread lost tape problem but it does paint a frightening picture. Bank of America, Citicorp, and Marriott are world class companies with sophisticated IT operations. How could these well-run organizations simply misplace their critical data assets?

Unfortunately, it's easy to make this mistake for several reasons. First off, the backup and off-site rotation procedure is full of manual processes, loose tape cartridges, unmarked boxes, loading docks, and 3rd party shipping. As boxes of tapes are transported from location to location they can easily get lost in a warehouse, delivered to the wrong location or simply disappear. It happens all the time.

Of course, this would not be an issue if organizations simply encrypted their backup tapes using a standard AES 128 or 256 bit algorithm. Without access to the encryption key, an attacker would have a chance of approximately one in a million million million of successfully breaking a 128-bit cipher with a brute force attack.

Given this level of protection, one would assume that security-conscious organizations would include tape encryption into their standard security defenses. Unfortunately, this hypothesis simply isn't true. In a survey of 388 storage professionals, ESG found that only 7% of users claim that they always encrypt their backup data while 60% say that they never do (see Figure 1).

Figure 1. Backup Encryption Frequencies



These broad market numbers are certainly disheartening so ESG decided to further examine the data, looking at backup encryption behavior by industry and company size. Regrettably, this study led to more bad news. Security-focused industries like financial services, healthcare and government agencies do not encrypt their backup tapes on a regular basis. When encryption habits are analyzed by company size, large enterprises are only slightly more apt to encrypt their backups than smaller firms (see Figure 2).

Why Hasn't Tape Encryption Caught On?

Encryption is a well-understood security defense that is used to protect data confidentiality and integrity throughout the enterprise. Network communication is commonly encrypted using an IPSec VPN when it is transported across an untrusted network. E-mail is often secured using the S/MIME protocol that supports encryption based upon the RSA public-key encryption technology. Many consumer banking and e-commerce sites use the ubiquitous SSL protocol to encrypt private information like account or credit card numbers between clients and servers. Since these encryption technologies are already an accepted piece of enterprise security, why hasn't backup encryption proliferated as well?

ESG asked storage professionals to identify their concerns about storage security. While this data is not specific to encryption, it does serve as a useful proxy. The data illustrates that users maintain a number of historical biases against storage security technologies like encryption. They tend to eschew tape encryption because they believe that:

- **Encryption does not come for free.** Users say they are concerned about the incremental cost of storage security. This was a legitimate concern in the past as backup vendors and 3rd party hardware appliances offered encryption at a hefty price. With the recent onset of high-speed crypto processors however, backup encryption pricing continues to slide rapidly each year. As a result, tape encryption solutions are becoming more affordable for large and small organizations.

- **Encryption can greatly impact backup performance.** Since encryption operations are processor intensive, users perceive that they will slow backup servers to a crawl. Again, this was true 10 years ago, but today's multi gigahertz microprocessors and specialized crypto chips can perform these

mathematical operations at wire speed with multi-gigabit encryption speeds are not unusual. Since these solutions also off-load encryption processing from server CPUs there is absolutely no performance impact. Complaining about encryption performance problem is now old school.

Figure 2. Tape Encryption Behavior Analyzed by Industry and Company Size

		Financial Services	Government	Health Care	Information Technology	Mfg.
"Does your company encrypt data as it is backed up to tape?"	Yes, always	6%	3%	3%	14%	5%
	Yes, frequently	7%	3%	3%	14%	11%
	Yes, but infrequently	9%	5%	11%	16%	13%
	No	65%	77%	67%	39%	56%
	Don't know	14%	3%	17%	16%	16%
	Total	100%	100%	100%	100%	100%

		Annual revenue $50 - $499 million	Annual revenue $500 - $999 million	Annual revenue $1 billion - $5 billion	Annual revenue greater than $5 billion
"Does your company encrypt data as it is backed up to tape?"	Yes, always	5%	15%	8%	4%
	Yes, frequently	8%	10%	9%	9%
	Yes, but infrequently	8%	10%	13%	14%
	No	74%	53%	59%	56%
	Don't know	5%	12%	12%	12%
	Total	100%	100%	100%	100%

- **Encryption adds complexity to restore processes and disaster recovery.** This is more misunderstanding than anything else. Encryption isn't the concern here, it is key management. A combination of a robust key management platform and good key management backup and storage processes can easily alleviate this concern. Fastidious storage professionals can certainly work with their vendors to add tape encryption while minimizing any disaster recovery impact.

New Business Requirements Demand Backup Encryption

To better protect data as it moves off-site, laissez faire backup encryption procedures are in dire need of a change. Over the next few years, this will likely happen. Why? ESG believes that several factors will make backup encryption far more common including:

- **Additional privacy regulations are coming.** The California Database Breach Act (aka CA SB1386) was the first state bill to mandate the disclosure of a suspected breach of consumer information. This law was first introduced in the California legislature in 2002 and has led to the increasing number of public disclosures. Since this bill took effect in 2004, similar legislation has been passed in Arkansas, California, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maine, Minnesota,

Montana, Nevada, New Jersey, New York, North Carolina, North Dakota, Ohio, Rhode Island, Tennessee, Texas, and Washington. At the federal level, Congress introduced over 12 bills addressing identity theft and notification of customers in the event of a data security in 2005 alone. During the summer, Senator Gordon H. Smith (R-OR) introduced the "Identity Theft Protection Act" (S. 1408). This bill would strengthen data protection safeguards and require customer notification if a breach of data security either caused, or posed a reasonable risk of, identity theft. Another example of data security legislation is a bi-partisan bill introduced by Representatives LaTourette (R-OH), Hooley (D-OR), Castle (R-DE), Pryce (R-OH), and Moore (D-KS) entitled "The Financial Data Protection Act" (H.R. 3997). HR 3997 also calls for strengthened data protection safeguards and a uniform, national standard for notification of data security breaches that would preempt all state notification laws.

- **More security threats and visible breaches.** Large enterprises must increase their security defenses over the next few years to combat a wave of new types of attacks. ESG anticipates new attack vectors targeting areas like backup software, IP telephony, web services, and Instant Messaging. Simply stated, the bad guys are looking for new easy ways to compromise critical systems and steal data. In this threatening scenario, backup servers and off-site tape shipments may become a prime target.

- **Encryption technologies baked into the storage infrastructure**. Two industry trends will lead to greater storage encryption proliferation. As described above, crypto processors are growing increasingly affordable daily so it is likely that more and more storage vendors will embed this capability into their systems. In addition, new security standards will alter the security features included in storage products. For example, the Fibre Channel Storage Protocol which includes encryption standards will be ratified by the ANSI T11 sub-committee early in 2006 and will quickly begin to appear in all sorts products. Storage professionals can also look forward to standards from the Trusted Computing Group, like the Trusted Platform Module (TPM) embedded in hard drives, to accelerate the implementation of storage security.

These trends will combine with a general increase in security awareness and spending across enterprise organizations in an effort to alleviate risks and improve corporate governance. In a few years, ESG expects that the backup encryption data will actually reverse – users that encrypt their backups will greatly outnumber those that do not.

Backup Encryption: Beyond Simply Scrambling the Bits

As encryption moves from an esoteric security offering to an everyday part of the storage infrastructure, many organizations will assume that their information is adequately protected. This is completely untrue; encryption should be looked at as a single layer in a defense-in-depth security implementation. What's more, new security must be as transparent as possible by not impacting existing business or IT with procedures. To truly protect the confidentiality, integrity, and availability of confidential information in an operationally efficient manner, backup encryption solutions should (see Figure 3):

- **Integrate seamlessly into the backup process and devices**. Backup processes tend to be well defined and under tight time limitations so backup encryption will not be well accepted if it demands process, equipment, or scheduling changes. To improve off-site rotation and data recovery efficiencies, encryption operations should be invisible to the backup software itself but well integrated with tape management utilities. For example, the tape encryption should be able to support tape duplication and media reclamation without sacrificing security.

- **Require a modest amount of training – not a CISSP certification.** There is no need to make storage administrators into security specialists or cryptographers. If tape encryption tools feature simple GUIs that resemble familiar storage and device management tools, storage managers can quickly assimilate tape encryption into their routines.

- **Support the security concept of "separation of duties."** This is important for two reasons. First, many shops will want to disconnect backup processes from security. This demands administration tools that support the concept of "role-based access control" so storage and security administrators can attend to v their individual duties with restricted access based upon roles and policies. Encryption tools must also protect encryption keys by limiting the number of individuals with access. Security best practices should also include separation of duties as a failsafe mechanism demanding that at least two individuals authenticate themselves to the key management system before being granted access.

Figure 3. What's Needed Beyond Encryption Alone

What's Needed	Definition	Why It's Needed
Seamless Integration	Include security in backup processes and technologies	▪ Ease the integration of security into storage operations
Ease-of-use	Simple administration and management of encryption, key management, and policy management	▪ Minimize training needs ▪ Minimize configuration errors ▪ Improve security ASAP
Separation-of-Duties	Restricting administrator access based upon identity and/or role	▪ Keep security and storage tasks independent ▪ Eliminate the "super user" role ▪ Provide checks and balances
Key Management	Key generation, rotation, protection, storage, and backup/recovery	▪ Protect encrypted data ▪ Secure keys against a rogue administrator ▪ Make sure keys are available for data restores and disaster recovery
Recovery Options	Multiple ways to use key management and tape drives to recover data	▪ Protect against obsolete hardware ▪ Link cartridges with keys especially for archival data ▪ Ensure that data can be decrypted after long periods of time.
Backup Media	Specific tape cartridges that can complement encryption	▪ Ensure against overwriting ▪ Help ease the process of matching media with encryption keys
Tape Compression	Apply a standard algorithm to reduce the size of tape data in order to save space	▪ Reduce media requirements as a complement to encryption

- **Include robust key management tools.** Key management is perhaps the most important but often overlooked component of strong encryption. Key management includes functions like key generation, rotation, storage, and backup. In terms of backup encryption, it is also important to remember that the data may sit in storage facilities for years. In fact, government regulations like HIPAA mandate the archival of certain patient information for 20 years or more. These complex requirements demand a key management system that can maintain an association between keys and media over time.

- **Offer flexible options for data restoration and disaster recovery.** Since encryption algorithms and tape technology changes over time, encryption solutions must provide ways to restore data regardless of the different generations of libraries. This again points back to key management and integration into the libraries. As long as the keys can be accessed, the libraries should be able to accommodate restores. As a last line of defense, decryption of tapes must also be provided through secure utilities.

- **Encompass the backup media.** As an additional security layer, encryption processes should also include the media itself. Best practices include barcode serialization to prevent duplication, and some media-based Meta data that can help guide IT managers to the right date ranges and encryption keys if barcodes are lost or altered. These media-based features help keep data secure while easing the efforts to match media and keys for data restoration.

- **Contain compression along with encryption.** One potential downside of encryption is that scrambling the bits can increase file sizes and thus consume more media. To alleviate this problem, tape encryption solutions should also include compression such that tapes are compressed, then encrypted.

Spectra Logic: Intelligent Tape Encryption

As previously stated, many storage and security companies are addressing the historical lack of storage security with new products, features, and services. One extremely interesting example of this new security focus comes from Spectra Logic, a pioneer in storage technology and management since its inception in 1979. In October 2005 Spectra Logic announced will integrate cryptographic capabilities into its tape libraries supporting the federal government standard AES 256-bit encryption.

This encryption capability alone is noteworthy, but several other tape manufacturers have announced similar strategies. Spectra Logic is unique however as it is the only manufacturer to integrate encryption (and key management) at the library rather than tape drive level. Other compelling features in Spectra Logic's offering include:

- **Endura Key Management.** Spectra Logic clearly did its homework and realized that strong key management will become a critical requirement for enterprise customers. Spectra Logic's Endura key management platform is a great start as it provides the right level of protection for both the keys themselves and access to the key management system. While keys are protected, each tape contains a "moniker" (similar to a nickname) that associates the media with a particular key. This can help users locate the right key without compromising security as no one actually sees the key itself. In terms of key management access, Spectra Logic demands two of three passwords. Again, this is an added level of protection eliminating the risk that one rogue employee can steal confidential data.

- **Seamless integration.** Spectra Logic integrated its encryption and key management with its existing BlueScale management software that encompasses its family of 8mm and half-inch tape libraries. Existing customers should be especially pleased with this development as it provides a single point of management for existing functions like library management, backup, and disaster recovery and now includes encryption and key management. Of course, Spectra Logic also supports role-based access control to enable the separation of storage and security administration tasks.

- **Ease-of-use.** Aside from the common BlueScale management look-and-feel, Spectra Logic wanted to make sure not to overwhelm its customers with complex security command-and-control. The company seems to have met its objective; security administration has been successfully consolidated into a few easy to understand menu options and commands. Spectra Logic deserves kudos here for easing administration without compromising the strength of its security.

- **Low cost.** This may be the best part of all. Spectra Logic customers with tape drives under support will receive BlueScale Encryption Standard Edition free of charge. The standard edition provides a single key for all encryption and decryption operations. Admittedly this is a modest feature set, but it may be enough protection for those customers who are only worried about the risk of lost tapes in transit to an off-site storage location.

Spectra Logic also offers its more advanced professional edition which enables the encryption of multiple tape partitions with independent keys. This edition contains some of the more advanced key management functionality described above and also includes tape compression for strong media utilization in support of encryption. In this way, Spectra Logic can certainly help its existing customers with basic (and free) protection or more advanced security functionality that fits a tiered storage or data classification model. Either solution should be attractive to security-conscious organizations of all sizes.

Bottom Line

It appears to ESG that the storage community is being dragged into security kicking and screaming but this behavior is no longer appropriate. It's time that the storage community woke up to the realities of encryption. Encryption isn't the draconian security domain it once was, it is becoming mainstream at the right time since business initiatives and government regulations make data encryption a requirement, especially for large regulated public and private organizations.

As backup encryption moves to the masses, it's important to look at the total solution, not just the cool crypto stuff. Tape encryption must fit existing skill sets, operations, and processes while supporting strong encryption algorithms, offering robust key management, and delivering flexible data restoration options.

When viewed in this light, Spectra Logic and its BlueScale Encryption seems to hit the mark. Spectra Logic is baking cryptographic capabilities into its libraries and supporting this security with the right management tools. As organizations begin to demand backup encryption, Spectra Logic certainly deserves a look-see.

The Enterprise Strategy Group, Inc.
20 Asylum Street, Milford, MA 01757 • 508-482-0188 • www.enterprisestrategygroup.com / info@enterprisestrategygroup.com