

## IBM Introduces Drive Level Encryption

**Date:** September 12, 2006  
**Author:** Heidi Biggar  
**Title:** Analyst

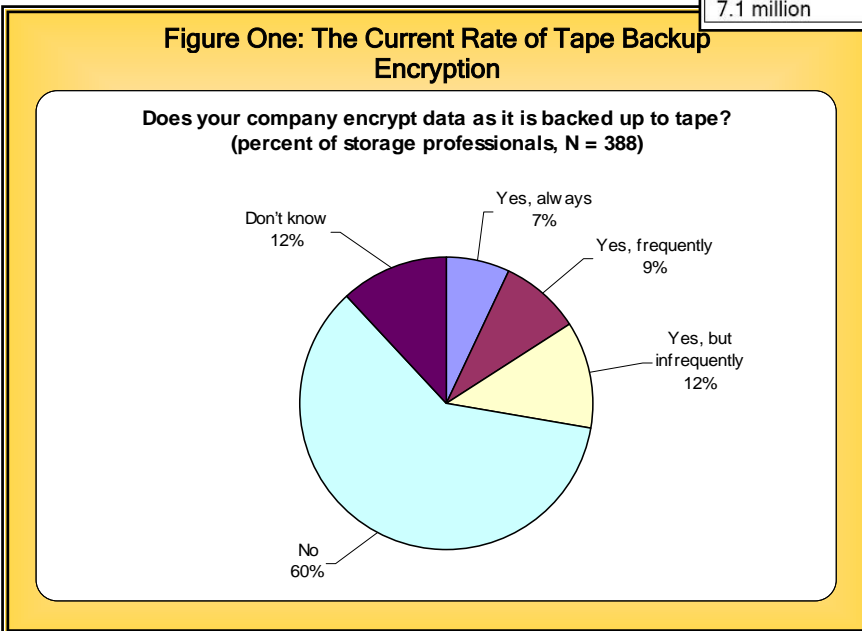
**Abstract:** Tape encryption isn't a household IT activity yet, but it is a necessity for many organizations today, especially those handling sensitive or private consumer data. Companies like IBM, with its new TS1120 encrypting tape drive and related products, are making it easier, more efficient, less expensive, and, dare I say, sexy, to encrypt data.

### The Proof Is in the Numbers

When it comes to the security of data residing on tapes, the numbers say it all: 18 publicly disclosed data breaches involving lost or stolen backup tapes containing the private data of more than 9 million Americans in the last 16 months (source: privacyrights.org). Three of these breaches involved high-profile U.S. banks and, more importantly, the private records of more than 7 million American citizens.

At an ESG-estimated cost of \$25 to \$150 per "lost" record for "damage control"-related activities (e.g., for notifying customers of the breach, providing credit protection services, and for changing account numbers), the potential financial impact of these breaches on these three organizations ranges from \$177M to \$1B. And this total doesn't factor in less-tangible costs such as damage to brand reputation, etc., which can be just as costly, if not more so, than the physical costs of the data breach – and, importantly, harder to fix and with longer-lasting effects.

Number of lost records resulting from three major tape loss/theft	Potential cost @ \$25 per record (low cost per record watermark)	Potential cost @ \$150 per record (high cost per record watermark)
7.1 million	\$177,500,000	\$1,065,000,000



With so much potentially at risk, why aren't more organizations encrypting data written to tape? Recent ESG Research points to two underlying factors:

- **Storage security is still a low priority:** Attribute it to naiveté or hypocrisy (we bet on the former), most companies – big and small – invest the bulk of their security dollars in the network perimeter, not infrastructure and application areas. ESG Research<sup>1</sup> finds that storage security, including technologies like backup tape encryption, continues to remain at the bottom of the Information Security priority list.

<sup>1</sup> ESG Research Snapshot Study, *Information at Risk: The State of Backup Encryption*, March, 2005.

Our Research finds that organizations – even financial services firms, banks and governmental departments that tend to be very diligent and savvy when it comes to security – often overlook vulnerabilities such as unencrypted backup tapes. However, this behavior is changing due to the increase in recent months of storage security breaches (as previously described).

- **Limited tape encryption options:** Historically, there have been three ways to do tape encryption – at the host, in software (e.g., in backup applications or storage utilities), or from an appliance (e.g., Decru, NeoScale, etc.). While these methods do work, each has limitations, which tend to become more pronounced as data volumes grow. These limitations include potential issues with performance, scalability, integration (i.e., lack of “transparency” to backup servers), etc.

By doing the actual encrypting of the data within the tape drive itself (a method referred to as “outboard” encryption) and creating a distributed encryption service, or what ESG describes to as an Enterprise Tape Encryption (ETE) environment, IBM addresses the shortcomings of existing technologies.<sup>2</sup> IBM also addresses the sticky issue of key management by creating a centralized key management application, or Encryption Key Manager. As for any performance degradation, IBM claims a less than 1% impact for its outboard process (for block sizes 6KB or larger). Data is first compressed and then encrypted.

And, lastly, IBM wraps new consulting services around the offering, which include policies and best practices for encrypting data, as a way to help customers with the fact that not all data needs to be – or should be – encrypted throughout its lifecycle. IBM also introduced new enhancements to its TS3500 library, including support for the new TS1120 drives, as well as a new virtualization engine, which is also expected to support these drives in the future.

### A Closer Look at the TS1120

IBM designed the TS1120 for optimal flexibility, allowing organizations to invoke and manage the tape encryption process in three different ways, depending on their environment. The three approaches are:

1. **System Managed Encryption:** Policies are managed at the system level. This option is available for both mainframe-attached environments using z/OS and for non-z/OS or non-mainframe-attached (i.e., open-systems) environments, though it is realized differently in these two types of environments.
2. **Library Managed Encryption:** Policies are managed at the library level according to logical volumes and serial numbers; this encryption is designed especially for non-mainframe environments. IBM’s new TS3500 library (formerly the 3584) supports the TS1120.
3. **Application Managed Encryption.** Policies are managed from the application or file-system level. Support for Tivoli Storage Manager to control TS1120 encryption is slated for the end of September. TSM currently supports software-based encryption. Generally speaking, ESG finds that end-users are not inclined to leverage software-based encryption tools such as those currently available with TSM. They tend to be performance hogs from a CPU-consumption perspective and can cause problems with the backup window.

All three methods support heterogeneous server environments (mainframe and open-systems), avoid host MIPS encryption overhead (in other words, they don’t consume host CPU cycles like traditional tape encryption options since the encryption process is done “outboard”) and can be implemented non-disruptively. Existing storage infrastructure as well as existing backup policies and procedures remain intact.

The first two approaches use the new IBM-developed Java-based Encryption Key Manager, or EKM, to centrally control key creation and the key store. And, in the case of Library Managed Encryption, a single instance of EKM can be used for key management in both z/OS and open-systems environments. When the EKM resides on the mainframe, it can leverage unique z/OS key generation and key store capabilities, including tamper-resistant hardware features. It can also use existing z/OS security management and DR procedures.

---

<sup>2</sup> ESG White Paper: *Enterprise Tape Encryption Requirements for the Banking Industry*, September, 2006.

## **The Bottom Line**

ESG believes IBM has the necessary experience with tape encryption (it has a long history with encryption in the mainframe environment) and industry presence to drive adoption of tape encryption technologies in general.

While ESG believes it makes sense to do encryption within the tape drive itself -- and sees a clear trend in this direction -- we suggest that organizations do a full backup security assessment before implementing any encryption technologies. That said, we believe tape encryption is widely underused.

It should be noted that though IBM is the first vendor to ship a tape-encryption-enabled tape drive, other tape drives and library vendors are expected to follow soon. Quantum, for example, is expected to support tape encryption at the library- and drive-level in the near future, and fourth-generation LTO drives are expected to ship with native tape encryption. Currently, Spectra Logic offers library-based encryption via its BlueScale technology and Quantum offers some security features with its DLT-S and DLT-V4 drives. But these technologies target a different market segment than IBM's TS1120, which is aimed directly at the enterprise.

Bottom line: With this series of announcements, IBM has made it a "no-brainer" for large organizations to make the decision to encrypt regulatory, private, confidential and business-critical data. The company also sets the tone for what we believe will be an active tape encryption season ahead.

---

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. and is intended only for use by Subscribers or by persons who have purchased it directly from ESG. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.