Enterprise Strategy Group

Information Security Brief

The Tape Encryption Opportunity

Date: August, 2007

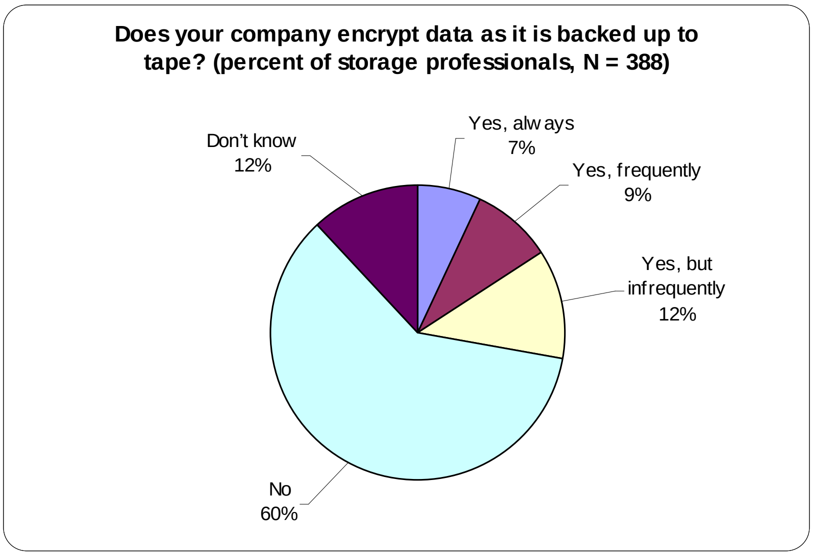
Author: Jon Oltsik, Senior Analyst

Abstract: While many large organizations are deploying tape encryption solutions this opportunity may seem a bit too tactical for big systems integrators. In fact, just the opposite is true. Helping customers scope and deploy tape encryption solutions may be one of those rare technology areas where short-term tactical implementations lead to long-term strategic projects.

Overview

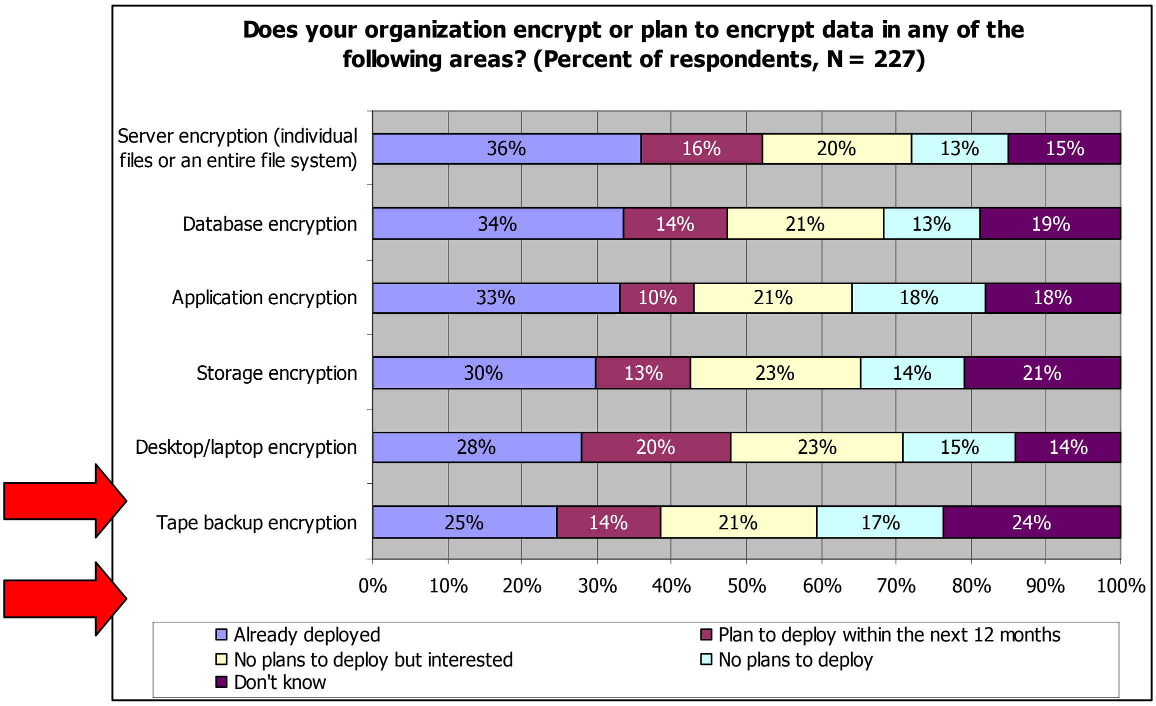
A few years ago, tape encryption was a non-starter. In a 2004 research project, ESG surveyed 388 storage professionals at enterprise organizations (i.e. organizations with 1,000 employees or more) about a variety of topics related to storage security. When asked if they encrypted data as it was backed up, only 7% of enterprises responded "yes, always." A startling 60% of storage professionals responded "no." The vast majority of data on tape was leaving data centers, being placed on trucks and then carted to some off-site storage facility in cleartext–the proverbial accident waiting to happen (see Figure One).

Figure One: Tape Encryption Practices 2004



What's taken place since our initial study? According to more recent ESG data, backup encryption has become much more pervasive in the past few years. When ESG Research re-visited this topic in 2006, we found that 25% of enterprises had deployed tape encryption solutions, 14% said that they planned to deploy tape encryption in the next 12 months and another 21% had no plans to deploy tape encryption, but were interested in the technology (see Figure Two).

Figure Two: Tape Encryption Deployment Plans 2006



The behavioral shift in tape encryption can be attributed to three critical factors:

1. **Visible data breaches.** In February 2005, a large financial institution lost a box of backup tapes containing the personal information of 1.2 million customers. The same thing happened in June 2005–only this time the tapes contained the personal data of 3.9 million customers. Estimating a per record cost of between $30 and $150, this would translate into a total cost between $1 billion to over $6 billion for the two breaches combined. Obviously, these incidents demonstrated that the risk was real.

2. **More and more privacy laws.** The granddaddy of U.S. state privacy laws is the California Security Breach Information Act. The Act may require organizations in some circumstances to publicly disclose certain kinds of information security breaches. A number of other states have followed California's lead and enacted similar regulations.

3. **Board room jitters.** When CEOs see data breach headlines emanating from brand name companies, they tend to be more than willing to open the corporate wallet to scramble bits on tape. Many tape encryption initiatives are corporate mandates rather than security best practices.

The Tape Encryption Opportunity

Yes, there has been a lot of progress, but the fact remains that 75% of the enterprises surveyed by ESG still don't encrypt their backup data. Some are still hung up on the traditional objections to any encryption–cost and performance. Enterprises may not have any budget dollars for backup encryption or they may feel that it will add too much overhead, slow down backup processing and throw a monkey wrench in an already tight backup window. Another obstacle to backup encryption is user confusion–encryption is still black magic to many storage professionals. Storage managers can quickly assume a "deer in the headlights" look when confronted with the choice of encrypting backup tapes using backup software, file system tools, crypto appliances/switches or encrypting tape drives.

Driven by data privacy requirements, it is likely that most large organizations will ultimately encrypt their backups, but they may need outside expertise to help them chart an appropriate course of action. Savvy service providers and system integrators will pounce on this opportunity by providing service offerings around:

- **Risk assessment.** Service providers can help companies sort through the combination of privacy legislation and internal backup processes to identify particular areas of risk. This exercise is more granular than it appears as it may span local and International laws and therefore require a backup audit on a facility-by-facility basis. The goal is to figure out which data is backed up, whether that data can be classified as "private," how it is transported off-site and where it ultimately resides. This type of assessment could lead to other systems integration or managed services opportunities. .

- **Backup strategy.** Before implementing a random tape encryption product, service providers can help customers define the right backup strategy for the future by assessing existing backup technologies, examining amortization schedules and reviewing backup architectures. Which equipment is due for an upgrade? Service providers can then compare existing backup processes and technologies with emerging business needs. Ultimately, these services can lead to strategic backup projects in areas like disk-to-disk backup, remote mirroring or redundant data centers.

- **Enterprise tape encryption.** Tape encryption can come in a variety of software, hardware and appliance offerings. The danger for customers is in implementing a potpourri of technologies that quickly become an operational challenge and a business continuity impediment. Service providers have the opportunity to work to define an enterprise tape encryption plan or strategy that meets security requirements and makes sense from a business and IT perspective.

Savvy CIOs will use the tape encryption requirement as a catalyst to look at storage technologies and backup processes across the enterprise. As such, service providers can find customers for a full spectrum of assessment, planning, implementation and managed services.

Tape Encryption Can Open Other Doors

Tape encryption and backup technologies are just the tip of the iceberg. The tape encryption requirement parallels other IT and business requirements around security, data privacy and regulatory compliance. In this instance, service providers may discover that tape encryption engagements cascade into additional strategic projects around:

- **Data governance and privacy.** Since the objective of tape encryption is protecting the confidentiality of classified data, questions around the data itself will likely arise. How is the data structured? Are there common data definitions? What policies govern data usage? How is the data classified? These questions can open a Pandora's Box around data modeling activities—and services opportunities—across the enterprise.

- **Regulatory compliance.** Growing interest in tape encryption is directly related to recently enacted state regulations requiring the public disclosure of certain data security breaches. Given this relationship, tape encryption engagements may quickly segue into broader discussions about compliance controls, best practices and monitoring tools. This is a perfect match—service providers offer expertise to large organizations needing help.

- **Security architecture.** An enterprise tape encryption architecture may dovetail well into other security areas. For example, retail and financial services companies may be implementing encryption technologies in POS systems, databases, file systems and networks. In this case, tape encryption may fit in with plans for PKI or symmetric key management. This is another area where enterprise needs exceed in-house skills—a good fit for external expertise.

- **Identity Management.** Data confidentiality technologies like tape encryption often raises obvious questions: Who has access to this data and what type of threat do they pose? When this discussion is focused on internal threats, the next logical step is to examine processes and technologies for user provisioning, access controls, management and auditing. In this way, tape management may act as a good catalyst for large organizations—and service providers—to light a fire under nascent identity management projects.

Partnering For Success

Service providers can only capitalize on enterprise inactivity and confusion around tape encryption if they have the right skills and technology offerings in place. One company that can help system integrators in this area is IBM. By working with IBM, service providers can complement homegrown methodologies and skills with a technology portfolio that includes:

- **Multiple tape encryption options.** IBM offers many technology choices for tape encryption. For example, mainframe shops can take advantage of an integrated CMOS cryptographic co-processor on z Series systems, while companies with other systems can take advantage of TS1120 encrypting tape drives. IBM's roadmap includes additional encrypting hardware and software in other systems, tape devices and storage systems.

- **Centralized key management.** This is another important area where IBM is taking a leadership position. Today, IBM offers its Integrated Cryptographic Service Facility (ICSF) as a component of z/OS for the management of symmetric and asymmetric keys. In this way, IBM's systems can help manage encryption keys and enable data sharing, archival and confidential transport and storage of tape media.

- **Integration choices.** IBM encryption solutions are designed to be extremely modular, allowing for flexible implementation. For example, cryptographic services are "callable" from mainframe storage facilities, Tivoli Storage Manager backup software or directly through device driver integration. This type of flexibility is critically important in addressing the diverse needs of a global enterprise.

The Bottom Line

In the near future, encryption technologies will closely mirror the old "death and taxes" cliché as one of those things that has to get done. About 25% of enterprises are already there, but the vast majority is still on the sidelines. Many of these firms lack the storage, security or enterprise architectural skills to move forward.

Service providers are in a perfect position to help here. While tactical implementation may be left to a local reseller, global SIs will still find plenty of opportunities to help large organizations align their storage, backup and security strategies with business requirements. IBM can certainly help service providers capitalize on these growing marketplace opportunities.