WHITE
PAPER

Protecting Confidential Data: The Role of Tape Encryption

By Heidi Biggar

September, 2007

Table of Contents

A Case for Tape Encryption

Protecting confidential data is nothing new to IT managers—they have been responsible for restricting access to corporate data and maintaining its physical security since the early days of computing. But in the last couple of years, it has taken on a whole new dimension—in large part due to the sheer volume of confidential data that is generated and moved around organizations today, the proliferation and tightening of corporate and federal regulations governing the protection of this type of data and the increasing number and visibility of data breaches often involving household name companies.

To put this in perspective, recent amendments to the California Database Breach Act (CA SB1386) alone have resulted in the public disclosure of more than 130 data breaches in 2005, leading to the exposure of the personal data of more than 55 million Americans. While the headlines in these cases included the banking and hospitality industries, the Act affected virtually anyone doing business with California residents.

What Is Confidential Data?

Much of the data we generate today is considered to be confidential in nature. As a guideline, ESG refers to confidential data as information that can be categorized as follows:

- Intellectual property
- Information that is protected by government regulations
- Non-public private information (NPPI)
- Information that is protected by industry regulations
- Information that is classified as company confidential or private

When you consider the multitude of other regulations corporations are subject to today (e.g., Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, FISMA and PCI/CISP to name just a few), the scale of the problem increases significantly—touching potentially every vertical market and every company, regardless of size or type, in one way or the other.

The Potential Financial Impact of a Breach

While it is impossible to calculate the full economic impact of these breaches, it is safe to say that it can be potentially devastating to the finances of the companies (and consumers) involved.

In general terms, the cost of a breach includes letters to consumers informing them of the breach, public relations costs, the payment of fines to applicable regulatory bodies and reparations—if any—to consumers whose personal information may have been used illegally. While these costs can be huge—in the millions of dollars, in some cases—the greatest cost may actually be tallied in damage done to the reputation of the organization(s) involved, especially if the breach gets broad media coverage. In fact, research shows that breaches like these can actually have an impact on the economy.

Data center conversations regarding confidential data protection still center more on devices with widespread distribution (i.e., laptop PCs and desktop PCs) than tape—and likely always will. But there is still a compelling case for tape encryption when you consider the tremendous amount of confidential data that is stored on it. Also, the availability of new, easier and more efficient methods of data encryption—and the promise of centralized key management solutions to ease that potential headache—should resonate with organizations and drive interest and adoption of tape encryption going forward. In March 2006, 25% of respondents to an ESG survey[1] said that they had already deployed tape encryption and another 35% said they hadn't, but were interested in doing so. The availability of LTO-4 encryption will likely serve as a key catalyst for change.

[1] ESG Research Report: *Protecting Confidential Data*, March 2006.

LTO-4 Encryption At-A-Glance

LTO-4 encryption-capable tape drives leverage industry standard AES 256-bit encryption in Galois/Counter Mode (GCM mode) or AES256-GCM in data center parlance. The encryption is done in the tape drive hardware—rather than software—at the drive level versus in an appliance. Doing so has several benefits.

- Encrypting in the tape drive hardware minimizes the performance overhead of the encryption process. By nature, hardware-based encryption is less compute-intensive than software-based approaches. Software-based approaches can put a burden on participating servers and can also make compression more difficult.

- Drive-level encryption is also more efficient than network-based encryption appliances from a processing standpoint. All of the encrypting is done "offline," after data has been ingested by the tape drive. It is not done "in-line" in the network—potentially causing a traffic bottleneck in the network and delaying what ESG refers to as the "Time to DR" process. This refers to the length of time it takes to get a copy of the data encrypted and off-site for DR purposes.

- There are also potential advantages to performing encryption at the drive-level (versus in the network) with regard to total cost of ownership (TCO), maintenance and training. Think about it. Encrypting in an appliance means more equipment to purchase, implement and manage. With drive-level encryption, this level of complexity and cost is reduced to just the price of the LTO-4 drive with encryption support. This feature is an option with LTO-4 tape drives.

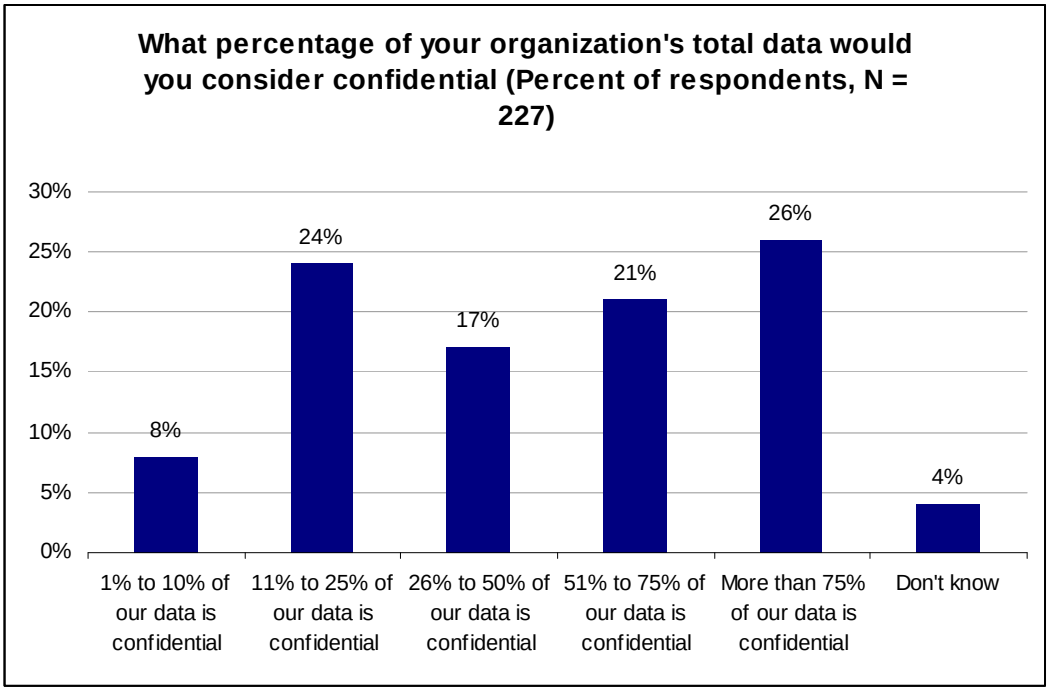
Is Confidential Data Ubiquitous?

One of the gating questions for whether or not organizations should encrypt data is whether there is a strong enough reason to do it or not. Our Research shows that there is—largely in part due to the huge, and growing, amounts of confidential data that organizations are generating.

Of the 227 respondents we surveyed, 47% believed at least half of their organizations' data could be considered confidential (see Figure 1). On average, databases contained the highest percentage of confidential data (54%)—followed by electronic documents (40%), e-mail/attachments (31%) and other unstructured data (24%).

What's driving this growth? One simple word: Compliance. When it comes to protecting confidential data, our Research shows that users are more concerned about regulatory compliance violations than they are about proactively improving security defenses. In fact, more than three-quarters (81%) of users say that government regulations were the biggest motivator for protecting confidential information. Sixty-four percent said they were driven to proactively identify and/or address security risks. Bottom-line: Security IS important, but it is secondary to satisfying regulators and auditors.

FIGURE 1. USER CONCERNS REGARDING ENCRYPTION

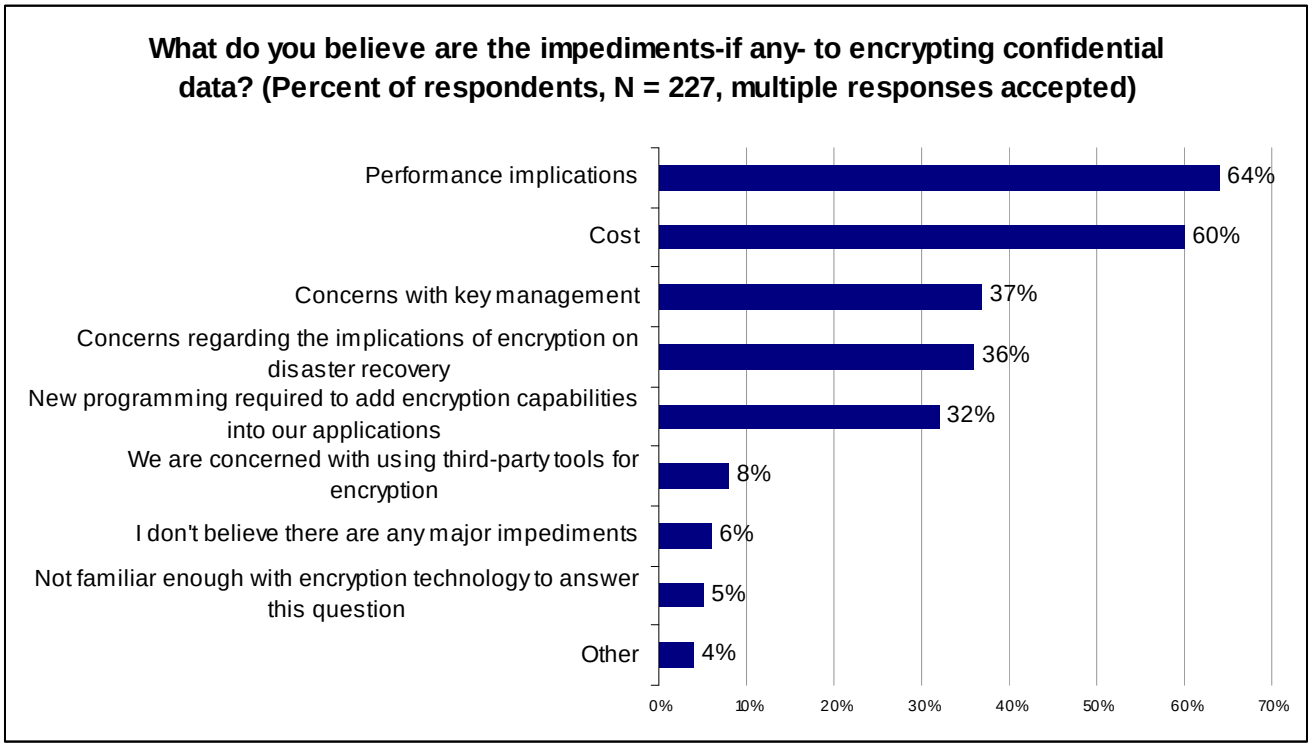


Source: Enterprise Strategy Group, 2007

There is still a great industry debate focusing on the best place to encrypt data. Should it be protected at the application layer, database layer, system layer or storage layer? If we're talking about tape encryption and it's done at the storage layer, should it be done in the network on an appliance, at the library level or in the tape drive itself?

Our Research shows that when users make decisions, they tend to be a function of convenience, risk analysis, technical trade-offs and budget concerns (see Figure 2). Further, they are generally leery about the affect encryption may have on system performance and the overall cost associated with purchasing and operating encryption technologies. When performing the encryption in hardware at the drive level using AES256-GCM, LTO tape technology appears to have addressed these major concerns.

FIGURE 2. IMPEDIMENTS TO ENCRYPTION ADOPTION



Source: Enterprise Strategy Group, 2007

Key Management

In the context of data encryption, perhaps no two words conjure up more interest in organizations than "key management." Key management is not widely understood or deployed among organizations today. It remains a mystery to most data center managers. Much like a lock on a door that needs a key to be opened, a key is needed to unlock encrypted digital content. Digital keys are typically made up of a hard-to-remember long string of characters or numbers. A key management solution simply provides a safe and secure place to keep track of digital keys.

As volumes of confidential data grow, and more and more data is encrypted across the data center, key management will become an important requirement—an absolute necessity from a management perspective. IT must manage all the keys for the data that's been encrypted and back them up as well. This applies to tape encryption in addition to data encryption on laptop or desktop PCs and other business machines.

ESG believes centralized key management holds the answer. Our Research shows that organizations are beginning to come around as well. Fifty-four percent of the users we polled said they were either extremely interested or somewhat interested in a centralized key management solution, while almost one-fifth said they had already deployed centralized key management[2]. In particular, we believe that products offering on-board encryption should include "hooks" for integration into centralized key management systems.

Users would like to make key management as seamless as possible throughout the enterprise. How these goals are actually accomplished (i.e., the route they take)—and the extent to which they centralize the management of all encryption—is up to individual key management providers.

[2] ESG Research, *Protecting Confidential Data*, March 2006.

ESG's View

The stakes have never been higher than they are today. As a result of disclosure laws like CA SB1386, a single lost backup tape can cost a company millions of dollars. In fact, ESG contends that protecting confidential data is a mission-critical requirement. LTO-4 tape encryption is a means toward that end with the potential for a number of user benefits (see Table 1).

TABLE 1. BENEFITS OF LTO-4 ENCRYPTION RECAP

Feature	Benefit
Encryption done in hardware	Minimizes performance overhead. Virtually no degradation to tape drive performance. Helps avoid burden on servers. Less compute-intensive than software-based encryption alternatives
Encryption done at the tape drive level	Allows for more efficient processing since processing is done offline. Can reduce "Time to DR" (versus in-line approaches). Reduces the amount of hardware that needs to be purchased, managed and maintained. No need for separate encryption appliance. Allows data to be compressed first and then encrypted, which helps maximize cartridge capacity.
Uses LTO-4 standard or WORM cartridges	Flexible support, depending on user environment (e.g., regulatory/corporate governance requirements).

The beauty of the LTO-4 encryption drive is that it makes encryption cost-effective and transparent (from an ease of use/deployment and performance standpoint)—and provides a roadmap for future generations of LTO Ultrium drives that are planned to include encryption. This is right in line with what our Research tells us users are looking for—and more importantly, what is keeping/has kept them from encrypting data that is stored on tape in the past (see Table 1). For these reasons, we believe tape encryption with LTO-4 products has the potential to become ubiquitous. Just like data compression, users can turn it on and let it do its magic.

ESG Research shows that encryption is taking a foothold in organizations and tape encryption is on the rise. The availability of LTO encryption should accelerate this adoption.

20 Asylum Street
Milford, MA 01757
Tel: 508-482-0188
Fax: 508-482-0218

www.enterprisestrategygroup.com