White Paper

The SMB Market is Ready for Data Encryption

By Mark Peters

January, 2011

This ESG White Paper was commissioned by Tandberg Data and is distributed under license from ESG.

Contents

The SMB Market, Security, and Encryption

Small to medium-size businesses (SMBs) are now facing many of the same security challenges larger businesses have faced for decades. Regardless of their size (since "SMB" can cover a wide range of operational sizes), virtually all companies in the space are in need of simplification to implement increasing security requirements, such as those laws and regulations mandating certain levels of protection for sensitive or confidential data. As is the case with large enterprises, data security is no longer an optional "nice to have" for the SMB market.

Until recently, SMBs have been less inclined—or able—to take the necessary steps to protect against data breaches for a number of reasons that typically include some or all of the following:

- Smaller security budgets
- Shortage of dedicated IT personnel
- Limited experience with or knowledge of security solutions

Some of these obstacles may have prevented SMBs from implementing new security technologies such as data encryption, the process of scrambling digital information to make it unreadable. Data can only be unlocked or decoded if a user, application, or device is provided with the required encryption "key." Encryption key management (EKM) is typically a software program that runs on a PC or server (either dedicated or shared) that provides the keys for the purpose of encrypting or decrypting data. All encryption users should remember that encrypted data is useless if the key is lost; it is critical that the encryption key database is backed up regularly and that a copy is also stored securely offsite. In short, it is absolutely true that *key management is the key to the successful use of encryption.*

While implementing encryption demands some effort, the mandates and motivations to do so are increasing. For instance, many countries have implemented laws requiring organizations to inform all affected parties if and when personal information is compromised. The costs of such a process are direct, but can also include damaged reputations and even additional penalties or—at the extreme—imprisonment. The good news is that *recent developments in encryption have yielded a mature set of solutions and made a very high level of data security much easier and more affordable to attain for SMBs*. Given the increasing criticality of data and data protection, the landscape and need for encryption (tape based or otherwise) is now moving beyond the enterprise and into the SMB market.

What Data Should be Encrypted

In order to comply with regulations or respond to the threat of potential data breaches, many SMBs are now implementing tape encryption for the storage of backup and archive data offsite. Approaches to this vary:

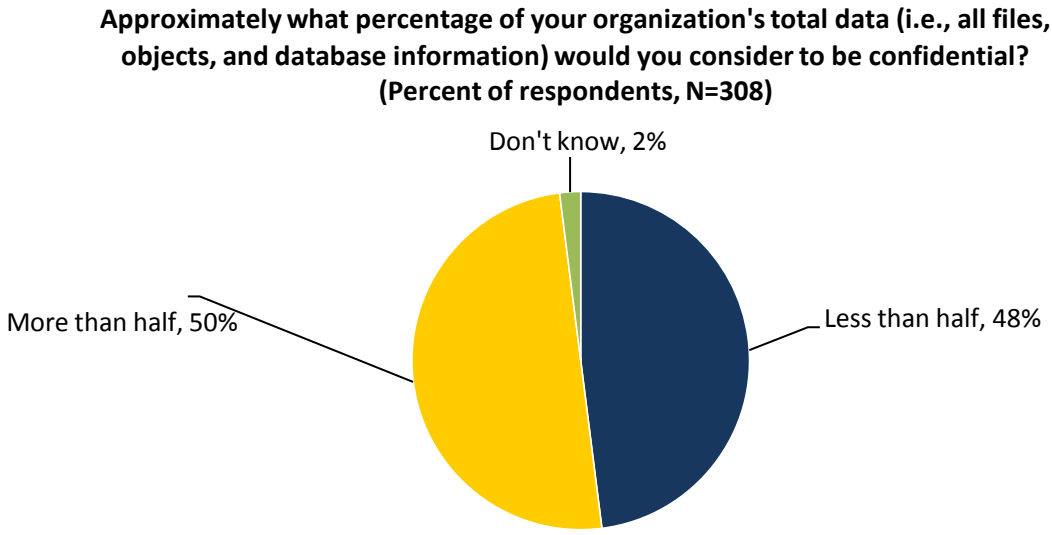
- For many users, the simplest—and certainly very effective—approach is to encrypt all data stored offsite; in their view, it makes no sense to attempt to decide what data should be encrypted and what should not be.
- Other users have decided to implement a tiered approach with their most highly sensitive data (in other words, data which would be costly or damaging to if lost) being encrypted first and other data being encrypted as appropriate to its confidentiality.

Users are certainly aware of the issue, as two pieces of ESG research demonstrate. ESG's 2011 spending intentions survey asked respondents to rank a multitude of "top IT priorities" through 2011 and 2012: for midsized companies (defined as those employing 100-999 people), "information security initiatives" were ranked *number two out of more than 20* priority activities.[1]

As to how much data is "confidential," ESG's research shown in Figure 1 indicates that half of all enterprises believe that more than half of their data falls into that category.[2]

[1] Source: ESG Research Report, *2011 IT Spending Intentions Survey*, January 2011.
[2] Source: ESG Research Report, *Protecting Confidential Data, Revisited*, April 2009.

Figure 1. Percentage of Organizational Data Considered to be "Confidential"



Source: Enterprise Strategy Group, 2011.

Even "confidential" data can be further classified; in practice, some businesses often choose to encrypt their *regulated* data first since managing the keys and the overall encryption process can become complex for large amounts of data. Depending on the amount, other businesses may want to consider encrypting just about everything in order to simplify the management challenges of classification and determining what to encrypt. New technologies continue to make encryption less expensive and easier to implement than in the past.

Encryption is also used extensively to protect archival data. Numerous government regulations and business practices often demand long-term records retention (periods of more than 20 years are not uncommon) and a growing amount of data will be kept forever. Since tape media is commonly used for data archiving, tape encryption can be utilized to keep the data confidential and tamper-proof throughout its lifecycle. In an archiving application, tape encryption must be supported with key management features built for the lifecycle of encrypted data.

In many industries, regulations often state how long data must be stored and protected, but in some industries these regulations also state that, after a period certain, data must be destroyed. This can create a problem if a user's data is all securely stored offsite as deletions (full or partial) can be time-consuming and expensive. However, by deleting the appropriate encryption key, the relevant data is effectively destroyed because it can never be read; interestingly, key deletion can be implemented as an effective management technique to control the lifecycle of data stored offsite.

Choosing Where to Encrypt

Once a user has determined the need for encryption, the next decision point is to decide where encryption should take place:

- At the server (processor)
- At the data path (switch or appliance-based)
- At the hardware (tape drive or disk drive)

Encryption and decryption are compute-intensive activities that can slow access to stored data, especially when storing and accessing large amounts of information. However, most servers average less than 30% busy, so encryption overhead may or may not be an issue depending on when it is used.

Although encryption doesn't help protect against device failures, worms, or viruses, it *does* address data loss, theft, intrusion, the growing spy-ware problem, lost PCs and personal digital appliances, or lost digital media (as confiscated data that is encrypted is virtually impossible to decrypt). Poor implementation of a tape encryption solution may result in over- or under- protected data, degraded application performance, or service interruption. Trade-offs certainly exist and, regardless of where a user chooses to encrypt, the key management process must be evaluated to determine which method will best work for any given business.

Methods of Encryption

It is now worth examining each method of—or location for—encryption in a little more detail:

Host-based/Software Encryption

With host-based encryption, servers encrypt data before it goes to the IO interface and device. Therefore, data is always encrypted in transit and at rest as it goes to and from tape or disk, making it possibly the most secure encryption technique. That said, host-based encryption uses host processor cycles that are potentially taken away from other host-based applications. This issue can itself be minimized by using a product/system that compresses data before it is encrypted, since—rather obviously—compressed data is smaller which reduces the bandwidth required to transfer it. Many existing or currently installed backup packages already offer encryption capabilities, thus avoiding any incremental costs. Host and appliance vendors should ensure that their products first compress and then encrypt data on its way to tape; however, it is advisable to always verify this since encrypted data is functionally uncompressible.

Standalone Encryption Switches and Appliances

With standalone encryption, all data passes through a switch or appliance that sits between the server and the tape or disk drives where it normally undergoes compression and encryption in the process. These special-purpose appliances are placed between the storage devices (normally tape and disk) and the server running the applications that are requesting encrypted data. The appliance encrypts all data going to storage and decrypts data going back to the applications—achieving this by monitoring all file access attempts. Unlike host-based encryption, encryption appliances protect data at rest, but not throughout the entire data path.

Tape Drive Encryption

Many tape drive manufacturers are implementing encryption via an ASIC in the tape drive, similar to the way tape compression was implemented in the mid-1980s*. Device-level encryption offers the highest performance levels.* In addition, compression has been a de facto standard on most tape drives for many years. Making the choice to encrypt data on tapes is invariably a fairly easy decision, especially if the cartridges are expected to be at all mobile and/or moving to offsite locations. Because the encryption capability is built into the drive itself, backup servers and networks don't experience any performance impact. Encrypting at the tape and disk drive level yields encryption for data at rest, but does not protect data in transit. Tape drive encryption is also proprietary, so having tape drives from multiple vendors can increase management complexity.

A few vendors offer library managed encryption (LME) to establish encryption policies and manage the transfer of encryption keys from the encryption key manager to the library tape drive(s). LME is typically found only in enterprise environments because it can prove expensive and complex and there can be compatibility issues between vendor drive types.

Most SMBs use a software application (typically backup software) to manage the transfer of encryption keys from the application to the tape drive or library tape drive(s). Encryption support for tape is included free with many backup software applications, making it the preferred solution for SMBs.

The use of tape is already well understood: tape is primarily used as a secondary storage medium for compliance and protecting data stored offsite (in case of, for instance, fires and floods). Tape is also use to reduce the overall cost of storage within data centres. It combines high capacity, a small form factor, reliability, and low cost of

ownership with a long shelf life (30 years is the number usually quoted). Tape forms the last line of defence in many disaster recovery plans because it is tried-and-tested and because it works. Tandberg is a reputable supplier of tape encryption products, which it enhances with interoperability testing, software certification (such as Symantec Backup Exec), and an extensive support organization.

Disk Drive Encryption

While RAID and mirroring policies can address hardware device failures, encryption attempts to address the problems of data loss and data theft by storing data in a useless (at least to anyone other than the legitimate user) format. In general, it is more difficult to decide which data to compress on disk drives. For disk drives used in response-time sensitive applications, drive level encryption can cause performance degradation and its impact should be carefully evaluated. Encrypting removable disk drives has the most compelling case, of course, since the drives are a form of mobile storage and hence more easily subject to loss or theft. Disk drive encryption is also proprietary and having disk drives from multiple vendors can increase management complexity.

Clearly, there's a lot to consider. While many users opt to encrypt at an application level, there are still the pros and cons of the various approaches to consider. Table 1 offers a quick summary guide to the inevitable trade-offs between the various encryption alternatives.

Encryption: A Decision Aid

Table 1. Summary of Considerations When Deciding on Which Encryption Approach to Employ

Location	Advantages	Disadvantages
Host-based software	• Lower cost method • Many existing backup packages offer encryption • Implementation often easier for SMBs • Protects data in transit and data at rest	• Increases processor overhead • Reduces data transfer times • All servers (local and remote) must run same software • Prevents lock-in with a specific hardware storage vendor
Switch or appliance	• Operating system-, server-, and storage device-independent • Heterogeneous protection across existing drives	• Usually higher cost • Increases number of appliances to manage as storage grows
Storage device: embedded in tape or disk drive	• Highest performance levels • Perfect for offsite data "at rest" • Server and appliance independent • Entire cartridge or drive encrypted • Scales linearly with each drive	• Proprietary solution • Not a solution for legacy tape/disk systems • Adds complexity when mixed storage vendors present • Only protects data at rest

Source: Enterprise Strategy Group, 2011.

The Bigger Truth

The growing number of security threats, continued economic uncertainty, and a steady number of both high-profile and publicly-disclosed breaches strongly indicate that the regulations for both government and industry data security requirements will only become more stringent. Security technologies like encryption provide the most value when they are implemented effectively and are integrated with ongoing IT operations. Put colloquially, scrambling data is proving to be easier than preventing its theft.

Encryption makes excellent sense for data stored on tapes, PCs, and any mobile appliances containing important information as this data is at high risk. More generally (as Figure 1 showed), organizations consider roughly half of all their data to be "confidential"—in other words, it is presumably worthy of protection even where that protection has not been legally mandated. As a result, encrypting data is steadily gaining momentum and expanding its reach beyond large enterprises and into the SMB market. As the value of data grows every day, users should expect the need to protect data with encryption to do the same.

Clearly, Tandberg Data is focused on delivering tape-based encryption solutions—but it also understands the broader necessity to publicize the need for encryption and encourage its adoption wherever necessary. As with any vendor committed to thought leadership, it knows that "a rising tide raises all boats" and (while not seeking charitable status!) it is in everyone's interest—at least anyone that has a bank account, buys anything in a store, has a cell phone, or conducts any business online—to promote the appropriate adoption and persistent use of data encryption.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com