

Best Practices to Secure and Protect Backup Data

DATA PROTECTION CHALLENGE

True story: *An IT administrator in a UK-based company steals backup tapes, one of which contained important data about the company's European operations. In an attempt to extort money, he anonymously alerts the company and demands a £275,000 ransom fee (approximately \$500,000 USD). The company agrees to the terms and arranges a money-for-tapes exchange while simultaneously working with Scotland Yard in a criminal investigation to discover the perpetrator. The British police prevail: they set up a sting, catch the data crook, and solve the crime. The tapes are returned to their rightful owner with no further damage.*

This “happy ending” security story sounds quite timely in the wake of recent security breaches at organizations like ChoicePoint, Bank of America, University of California at Berkeley, Lowe’s and a litany of others. Surprisingly, an IT staffer at Imperial Chemical Industries (ICI) carried out the data theft described above in 1977 – nearly 30 years ago! This story illustrates that information security breaches and backup tape theft have been undesirable ramifications of business computing since its inception. Basic criminal behavior like extortion and theft is a few years older still.

While computer-based criminal activity may not be a new problem, there is no denying that illegal activities in this area have become far more pervasive over the past few years. According to the CERT Coordination Center (CERT/CC), a U.S. government-sponsored security organization at the Software Engineering Institute (SEI) of Carnegie-Mellon University, the number of reported security events rose from approximately 21,000 in 2000 to more than 137,000 in 2003 – and CERT estimates that for each reported event, approximately four events go unreported (see Figure 1).

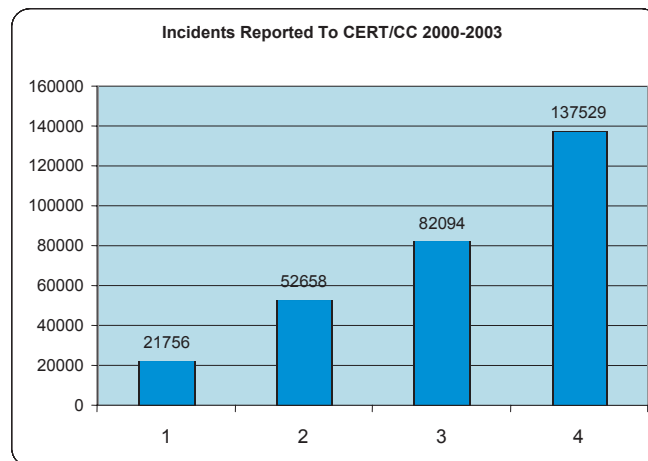
CONTENTS

Data Protection Challenge	1
Best Practices for Secure Backup	6
Methodologies for Encryption	11
Summary	15
Myths, Realities and Advice on Secure Data Protection	16

In partnership with:



This paper is a collaboration of industry experts in the analyst, consulting, implementation and storage business for all forms of information assets.

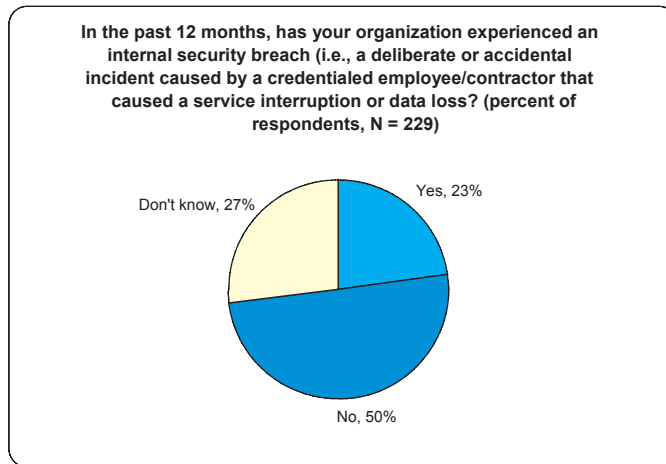
Figure 1: Security Incidents Continue To Escalate

Source: CERT/CC and Enterprise Strategy Group

Why have information security breaches and data theft become so pervasive? Several reasons:

- **There's money to be made.** As the story goes, when the famous bank robber Willie Sutton was asked why he robbed banks, he responded, "Because that's where the money is." Today's cyber-criminals recognize that confidential data and identity theft can be very lucrative businesses. Even at 10 cents apiece, stealing 5,000,000 credit card numbers can result in a hefty payday of \$500,000.
- **Data tends to be porous.** To bolster productivity, organizations across the globe poured billions of dollars into new applications, computing devices, storage capacity, storage devices, and network infrastructure over the past few years. Unfortunately, many firms minimized or disregarded the security implications of all this new technology, leaving their confidential data "an easy mark" for more sophisticated cyber crooks.
- **Confidential information is easier to get to than ever.** Corporations (rightly) believe they are taking the proper precautions to protect their data by sending it off-site to a secure location for disaster recovery purposes. However, in performing this process they forget to properly secure the information first.
- **Anyone can do it.** Systems containing confidential data that were once protected in locked data centers are now accessible to anyone with an Internet connection. Yes, this data sits "behind the firewall," but perimeter security simply does not provide enough protection. For example, in a 2005 ESG research survey 23% of security professionals admitted that their organization had experienced an internal security attack (i.e., an attack carried out by a credentialed employee or contractor) in the previous 12 months (see Figure 2). Of those that said they had experienced an internal attack, 38% said that it resulted in "data corruption or loss." At the same time, external hackers have grown more sophisticated and common hacking tools for slipping through the firewall are readily available on the World Wide Web.

Figure 2: Internal Threats



Source: Enterprise Strategy Group

Data Security Has Become Business Critical

CEOs are starting to understand the impact security is having on their businesses. These executives realize that minimizing information security requirements can lead to damaging headlines, public scrutiny, and customer relations nightmares. In addition, government regulations like the Health Insurance Portability and Privacy Act of 1996 (HIPAA), the Fair and Accurate Credit Transaction Act of 2003 (FACTA), and the Financial Services Act of 1999 (aka Gramm-Leach-Bliley or GLBA) mandate controls and audit requirements to protect consumer and confidential data. Organizations that fail to comply can face stiff fines while executives themselves could end up in jail (see Figure 3).

Figure 3: Penalties for Non-Compliance

Regulation	Potential Penalty	Potential Fine
GLBA	10 year prison sentence	\$1,000,000
HIPAA	10 year prison sentence	\$100 fine with a maximum of \$25,000 per year
Sarbanes-Oxley	10 year prison sentence	\$15,000,000
SEC Rule 17a-4	Suspension	\$1,000,000

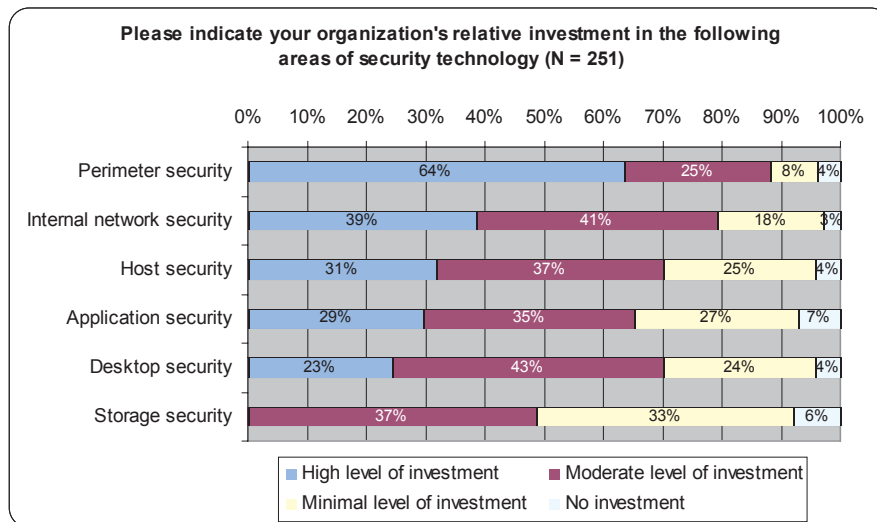
Source: Enterprise Strategy Group

To address data security shortcomings, risk-averse CEOs are now more willing to prioritize data security protection and invest accordingly in security technology countermeasures. A Morgan Stanley CIO survey illustrates this point, as CIOs selected information security spending as their top priority for the next 12 months.

In spite of this security focus however, data remains vulnerable. Why?

- **Security investment remains focused on the network perimeter, not the data.** Many organizations are still focusing on traditional security problems instead of new threats. For example, a 2005 ESG survey illustrates that users continue to invest heavily in perimeter devices (i.e., firewalls and gateway appliances) that inspect network packets rather than safeguards for business critical systems and data (see Figure 4). As previously stated, perimeter security provides minimal protection for private and confidential data.

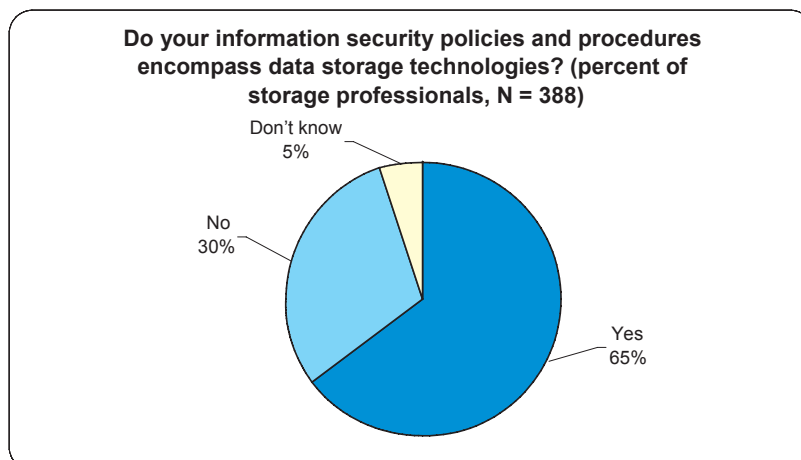
Figure 4: Perimeter Security Investment Remains Highest



Source: Enterprise Strategy Group

- **Storage remains insecure.** ESG data suggests a frightening reality: the storage infrastructure that houses private data is extremely insecure. In fact, 30% of users do not include storage infrastructure in their corporate security policies and procedures (see Figure 5). While servers provide some storage protection, an inside attack could easily result in compliance issues, intellectual property theft, or data corruption that could be devastating.

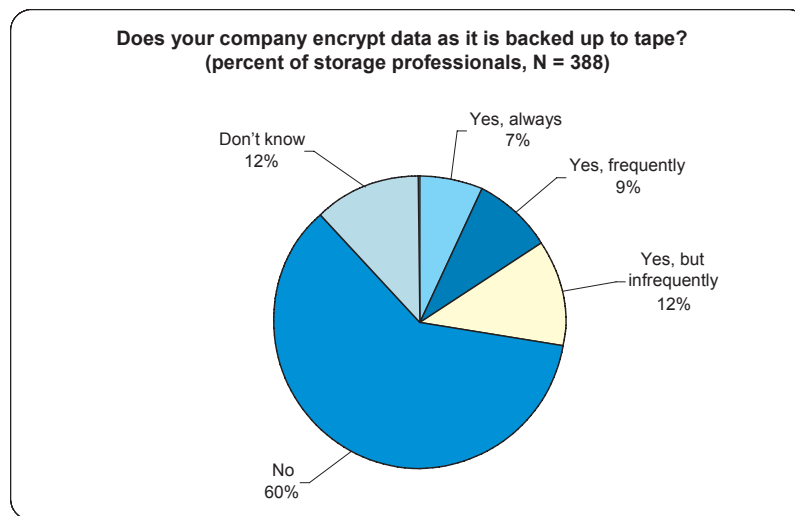
Figure 5: Storage Security Is Still An Island



Source: Enterprise Strategy Group

- **Backup encryption is virtually ignored.** Almost all organizations back up their data regularly and maintain off-site copies for data retention and disaster recovery protection. In spite of the fact that backup tapes contain private (and regulated) data and are often transported by commercial delivery services via public transportation, most companies don't encrypt their backup tapes. Sixty percent of users claim that their organizations never encrypt their backups (see Figure 6). This is even true in "security-conscious" industry sectors like financial services (65% never encrypt backups), government (77% never encrypt backups), and healthcare (67% never encrypt backups).

Figure 6: The Current Rate Of Backup Encryption



Source: Enterprise Strategy Group

The common understanding is that building an end-to-end security infrastructure is a lengthy project that will take years to complete. This is compounded by the fact that the lack of backup encryption is puzzling as this problem can be solved through a number of proven solutions. As a result, users continue to eschew backup encryption and many IT professionals maintain erroneous beliefs about encryption technology: the common understanding is that building an end-to-end security infrastructure is a lengthy project that will take years to complete. This is compounded by the lack of backup encryption, despite the fact that this problem can be solved through a number of proven solutions.

BEST PRACTICES FOR SECURE BACKUP

Backup encryption should be one of many activities that formulate a comprehensive security strategy. In many environments, storage has operated outside of the realm of security officers for some time, as their main focus has been primarily on areas such as perimeter security, intrusion detection/prevention and protection of host systems. As a result, the storage infrastructure – both primary storage and especially copies of primary storage – is likely to be an Achilles' heel when it comes to security. Policies for data security are a corporate concern and should be a fundamental element of an enterprise security strategy. Strategic security policies can then spawn tactical and operational policies through the joint efforts of the security and storage organizations. To that end, storage must become an integral part of the corporate security strategy.

To achieve these goals, a corporation should build a practice around five fundamental areas:

- Assign accountability, responsibility and authority
- Assess risk
- Develop a data protection process
- Communicate the process
- Execute and test the process

1. Assign accountability, responsibility and authority.

Make storage security a function of overall information security policies and architecture. Even if companies decide that backup or storage security responsibilities should reside within the storage team, they still must integrate any storage and backup security measures with those that secure the rest of the infrastructure. This will help build defense-in-depth protection.

Separate duties where data is highly sensitive. It is prudent to ensure that the person authorizing access is not the person charged with responsibility for execution.

2. Assess storage risk as it pertains to information security.

Perform a risk analysis of the entire backup process. Managers must examine each step of their backup methodology looking for security vulnerabilities. Could a tape administrator secretly create copies of backup tapes? Are boxes of tapes left out in the open? Is there a tight, end-to-end chain of custody for your backup tapes? If data is backed up and transported in clear text, vulnerabilities like these could make mission-critical data easy prey.

Execute a cost/benefit analysis on backup data encryption. If a risk analysis exposes numerous vulnerabilities, organizations should seriously consider whether encryption is warranted. This project should go deeper than software licensing or device cost alone, and include the costs of encryption-related operational tasks in backup and disaster recovery processes. The total cost of encryption should be compared to potential risks and the likelihood of a security breach to determine whether it makes economic sense to implement encryption broadly, narrowly, or not at all. Given the series of recent publicity, tape encryption of sensitive data is a worthwhile investment.

Identify sensitive data. Know what files, databases, and columns are considered sufficiently sensitive by the business units to warrant the additional cost of protection. Additionally, know where your data resides. Many times data is duplicated throughout the environment. It is important to have policies and procedures set up so that there is a good understanding of where data lives at any point in time. For example, companies have information on laptops that may also exist in duplicate on a network drive or in a backup repository used by the PC.

3. Develop an information protection program that ensures the security of a corporation's information, regardless of where it is at any point in time.

Adopt a multi-layered security approach.

Adopt a multi-layered approach to data protection by taking best practices that may already exist for the data network and applying them to the storage network, while adding layers unique to the characteristics of data at rest. These include the areas of:

- **Authentication:** Apply multi-level authentication and anti-spoofing techniques.
- **Authorization:** Enforce privileges based on roles and responsibilities versus full administrative access. Where available, leverage role-based administrative capabilities of storage management applications — especially backup.
- **Encryption:** All sensitive data should be encrypted when it is stored or copied. In addition, all management interface data transmitted over any non-private network should be encrypted. Sensitive data is usually defined as information containing either personal information or trade secrets.
- **Auditing:** Logs of administrative operation by any user should be maintained to ensure traceability and accountability.

Copy your backup tapes.

Depending on a single copy of data is never a good idea. While tape media can have a long life, it is susceptible to environmental and physical damage. A common practice is to perform nightly backups, then ship those tapes off-site – with no verification process. The recommended best practice is to copy backup tapes and then send the copy off-site. The advised method of copying backup tapes is to write a new tape by reading the original tape. This has the benefit of both verifying that the backup data is readable as well as eliminating the single point of failure of the backup tape.

The reason most often given for not having a tape duplication policy is lack of time. From a practical standpoint, backups take too long, and it is impossible to duplicate the data in a timely fashion. There are two methods of addressing this issue. The first method starts with optimizing the backup system to decrease the amount of time it takes to complete the original backup. Once this is done, multiple high-speed tape drives can be used to create the second copy for off-site purposes. The second method is to use the ability of some backup software packages to create both an original and a copy simultaneously. While this method does not have the verification benefit discussed in the previous paragraph, it allows people to immediately make copies – and any type of copy is better than no copy. Regardless of the size of your environment, a combination of high-speed tape devices, virtual tape libraries, and professional services can help meet this important requirement.

Implement a tight, end-to-end chain of custody process for media management.

Chain of custody refers to the act, manner, handling, supervision and/or control of media or information (usually, but not always, tape). The ultimate goal of successful chain of custody is to preserve the integrity of the resources. The following should be considered concerning chain of custody.

Removable media should be tracked by bar codes and reports should be generated detailing the current location of the media. A best practice is to report daily on tapes that are to be sent off-site, and those that have expired and should be retrieved from offsite storage to be recycled or destroyed. Documented standard operating procedures should be in place to ensure that these measures are carried out.

The off-site location and the process that is used to access the off-site storage should be analyzed for security practices. Media should be placed in locked tubs before leaving the data center and subsequent tracking done at the “tub” level. Tracking should be performed by scanning bar codes every time a tape tub is moved, including at data centers and at off-site locations. Tubs of media should be signed for and never left exposed for someone to take.

Reconcile the inventory of media that is stored off-site on a regular basis (at least monthly) with tapes that may be kept in house. At the end of each month, a physical scan of the off-site storage should be compared to the records of the backup/archive application to discover inconsistencies. If media is not accounted for, then appropriate steps must be taken.

Once the media has reached obsolescence or can no longer be relied upon for its integrity, the media must be appropriately destroyed. The destruction of magnetic media is usually accomplished by applying some destruction process to the cartridge, either scrambling the data on the tape or destroying the tape all together, rendering it useless. Department of Defense standards, for example, call for erasure of tapes containing confidential information, and destruction via fire for tapes containing secret and top secret information. Erasure can be performed on-site with the proper degaussing equipment, or via a third-party erasure service. (If performing erasure on-site, ensure that your degaussing equipment is rated for the type of media you are erasing.) Destruction is best performed via a third party that provides a certificate of destruction.

Encrypt all data that contains sensitive information.

The final and perhaps most critical layer of a multi-layer protection strategy is data encryption. If all your other defenses have been compromised, effective encryption renders the data unusable to unauthorized individuals. While encryption capabilities have been available for some time, few organizations have taken advantage of them. This is due in part to a lack of appreciation of the actual risk as well as the fact that some solutions have technological limitations can make encryption impractical. Awareness of the risk is no longer an issue, so let us focus on the technological concerns.

As discussed previously, security of storage has not been a priority for most organizations, and storage administrators have traditionally focused on convenience and manageability rather than security. When considering encryption specifically, the practice of encrypting information that travels over publicly accessible networks is standard procedure today. The use of virtual private networks (VPNs), secure Web sessions for sensitive transactions through secure socket layer (SSL), and secure login sessions via secure shell (SSH) are examples of encryption in use by millions of people every day.

However, these are all examples of securing *data in transit*. The focus is on preventing someone from unauthorized snooping as data travels from point A to point B. The issue of securing data at rest, whether it resides on disk, tape, or optical media, is a more recent concern. Data encryption can occur at the application, database, operating system or network level. In addition, for media shipped off-site, backup vendors also provide encryption capabilities. The final section of this paper examines these approaches.

Understand your data's chain of custody process.

Another critical element in secure media handling is to ensure that the off-site storage vendor also follows best practices. Here is a baseline of some things to consider.

- **On-Site Vulnerability**

Don't leave tapes in an unlocked container (like an open cardboard box) on the receptionist's desk to await pickup. Pick up should be a standard operating procedure in which a responsible IT person hands over and receives a signature from a known (ID carrying) vendor representative.

- **Background checks**

The company is going to be storing your critical data, so you must ascertain the company conducts background checks on every one of its employees.

- **The company should have a complete chain of custody process that utilizes bar coding to ensure tracking of individual tapes and cartons/tubs of tapes when they are rotated or in transit.**

Talk to the off-site service vendor about the entire process of how media is handled from start to finish. Look for an emphasis on physical security, and audit and control mechanisms to ensure that the process is being followed. It is inadvisable to move sensitive data from point A to point B in a vehicle emblazoned with the vendor's name, easily identifying it as carrying sensitive data.

- **Container vaulting**

Container vaulting is when you send a company a tub/box of tapes, and they track only the tub/box. Most off-site service vendors support this type of vaulting.

- **Individual media vaulting**

Individual media vaulting is when the off-site service vendor is shipped a tub/box of tapes, and they track each piece of media in the tub/box. The vendor should support this type of vaulting.

- **Physical security controls**

Facilities should be appropriately secured. No unauthorized person should be able to gain access or enter the vaults.

- **Environmental controls**

Tapes and other media should never be stored in a vehicle's trunk, or any other non-environmentally controlled location. If a vendor is going to be storing tapes, the environment must be strictly controlled, including temperature, humidity, and static control. Dust is the enemy of most media and media recording devices. To a magnetic head, a particle of dust is like a boulder on the freeway to an individual in a car. The backup and archive environment must remain clean and dust free. A soft, static-free cloth should be used to clean the outside of cartridges and dust should be removed from slots of a library or storage rack by using compressed air from a spray can. Tapes should be shipped in an electrostatic holder in a tub and not piled into a tub or a cardboard box. Although appearing quite durable, tapes can be easily damaged by being mishandled.

Consider Electronic Vaulting.

One thing to consider is to vault data electronically and bypass the need to send the information on physical media in a vehicle. There are a number of companies today that offer IT professionals the ability to backup data over the Internet. The data can be encrypted and moved via the Internet to a secure backup data facility. This may not be a practical solution for all of a company's data, but it may be practical for data that is distributed on file servers or personal computers. This data can represent 60% of a company's information and is challenging for IT to control.

Make sure that the vendor offering these services encrypts the data while being transferred and when it is at rest. This means that companies should take the time to segment their data and send only the most critical data, which they would not want to transport on tape media via truck or over the Internet. Additionally, discuss with the vendor how the information is kept available. Is it backed up to tape? Is it replicated to another site? Ensure that the vendor's disaster recovery practices meet an exceptional standard. Discuss with the vendor how the information is kept available for recovery or litigation support.

4. Communicate the processes that are to be taken around information protection and security.

Now that the process has been defined for ensuring that the sensitive data is properly protected and handled, it is important to ensure that the people who are responsible for carrying out its security are informed and trained. This is the most important aspect of item 1, which is to assign accountability, responsibility, and authority.

Inform business managers of risks, countermeasures, and costs. Data loss and intellectual property theft are a business issue, not an IT issue. As such, the Chief Information Security Officer (CISO) should begin a data security effort by educating business executives on risks, threats, and potential losses from security breaches, plus the cost of various security countermeasure options. In this way, corporate officers can make informed decisions on the cost/benefit profile of data security investments.

Assess risk and train staff. ESG's data clearly demonstrates that "an ounce of prevention is worth a pound of cure." In other words, organizations that assess risks and train staff are more likely to implement security policies, procedures, and technologies that protect vital assets. On the other hand, vulnerable infrastructure and unskilled staff are a problem waiting to happen. If anything, this data points to a real payback for doing the security "grunt work."

5. Execute and test the information protection security plan.

Secure data protection is not about technology; it is about process. That's why it is important to test the process. Additionally, as a company grows, information and data protection needs change, so the information security practices must change as well. Once the end-to-end plan has been developed, defined, and communicated to the appropriate people, it is time to begin execution. Ensure that the tools, technologies and methodologies that need to be deployed for information classification are in place. This may mean deploying new technologies that allow information to be classified or tagged with meta data such that, upon backup, the information is backed up using the right rules and processes.

Test the process once it is in place. Remember, the process to be tested needs to include both backup and recovery. Attempt to inject any conceivable threat into the process including server and tape loss, network issues, device issues, data classification issues and any other scenario that might affect the business. Test with people who may be less familiar with the process. This can help ensure that the process is easy to follow and can be executed if the usual person is unavailable due to illness, vacation, or termination.

METHODOLOGIES FOR ENCRYPTION

A large segment of this white paper discusses the fact that data should be encrypted before it is put on tape. Below are some methodologies for encrypting data.

Application/Database encryption

Database applications offer both native and third-party tools that can encrypt sensitive tables, rows, or columns within tables to ensure that the data is viewable only by users specifically authorized to see those elements. Fields such as credit card numbers, employee salary information, and personal medical data are often encrypted in this way. The advantage of application-based encryption is, of course, that it is tightly coupled with the application itself. It encrypts only the data that needs to be encrypted, thereby minimizing overhead. It also has the advantage of encrypting data at its origin, providing an even greater level of security.

Operating system encryption

Modern operating systems also incorporate the ability to encrypt data stored within a file system, directory, or individual file. For example, Microsoft® Windows® XP provides an Encrypting File System that supports public key encryption and is fully integrated with the operating system. Encryption at this level can be very flexible and applied to a wide range of data. The potential downside is CPU overhead and file system performance as data must be decrypted to be accessed. Key management is another concern, as will be discussed later.

Network encryption devices

At the network level, a new breed of hardware security modules (HSMs) have emerged that can provide a transparent level of data encryption. These appliances can sit on either a SAN or LAN and provide encryption at wire speeds to either some or all of the data that travels on the network.

These devices have several advantages that make them worthy of consideration. First, they are fast. One of the major roadblocks to enabling encryption is performance (see the discussion of backup encryption below). These network devices not only perform encryption at wire speeds but also introduce minimal latency to the environment.

Second, they are versatile. Depending on the organization's specific encryption requirements and network architecture, there is likely a device that will meet its needs. Various devices are optimized to support a variety of host systems, network protocols, primary storage, backup, and even application-specific requirements, such as database field encryption. Residing at the network level, these devices can often be managed with little or no impact on host systems or applications.

Third, they are relatively inexpensive. Given the risk of privacy exposure or loss of proprietary information, the return on investment of these devices can be compelling.

Encrypting through backup application software

With regard to backup specifically, most major backup applications offer encryption either as a standard or optional component of their product. Let's examine how this works.

An enterprise backup application typically consists of several components:

- A central server that maintains a database of all of backup configuration information, such as backup clients and their schedules, and administrative components of the environment. In addition, it stores the history of all backups, allowing those backups to be searched for restoration purposes.
- One or more servers that manage the creation of and access to backup media (either disk or tape).
- The systems whose data is actually backed up – the backup clients – who transmit data to the servers to be processed.

Traditionally, data and metadata is sent in cleartext between the systems involved in this process and no encryption is performed. The exception, in most environments, is usually when a remote backup service provider is used rather than an in-house operation. Because this data is sent over an external network, it is common practice for third parties who provide backup services to employ network-layer encryption to ensure data privacy and integrity while in transport.

For an in-house operation using an enterprise backup application, a typical approach to employing encryption might consist of:

- Enabling encryption within the backup application
- Transmitting the encrypted data to the appropriate backup server on to tape or disk

There are several reasons this is not common practice. First, the processing impact of performing host-based encryption on a production environment can be substantial. In an active environment, where critical business functions are being performed on a 24-hour basis, this overhead may be overly intrusive. Second, the encryption process can slow the rate of data being transmitted to the backup host and then subsequently to tape. Modern tape devices have very high throughput rates and require a constant stream of data to perform in an acceptable manner. When the data rate drops to a point below the streaming requirements of the device, performance dramatically falls. Essentially the tape device must stop, backup, and restart. When this happens repeatedly, “shoeshining” occurs, resulting in very poor performance and quicker tape wear. Third, encryption of data has the side effect of “flattening” a file, i.e., making it less compressible. Modern tape devices perform compression and most environments depend on compression to minimize the number of tapes required for a nightly backup. Compression also impacts performance, since compressed data represents fewer actual bytes that must be written to tape. While it is possible for backup applications to compress data at the client side, as with client-based encryption, the performance implication on production systems can be unacceptable.

The final and possibly most critical reason that encryption has not been more widely adopted for backup data has to do with the management of encryption keys. An essential element of the process of encryption and more to the point — decryption — key management is mission critical. Restoring encrypted data is impossible without the key and having a process for administering, protecting, and recovering keys becomes an essential parallel process for data recovery.

Encryption key management

All current encryption products use a variation of private key cryptography. The loss of a key, or of the encryption product in use, would cause the loss of all encrypted data.

As discussed above, encryption is critical to data management, especially long-term storage of offline data. No alarms might sound if a backup tape is stolen and read, and these tapes may contain consistent copies of entire data sets. In fact, without encryption, backup tapes are normally completely insecure. However, encryption can turn the tables on security, locking your own data away from your use.

Consider encrypted data on tape as being locked in an indestructible safe sitting out on the street. The keys to that safe are securely held in your pocket, so you can access that data if needed. Nevertheless, what happens if you need to share those keys with someone else? Once they get away from your control, they can be duplicated and your data can be read. In addition, what happens if the keys are lost?

Key Management Best Practices: change keys, prevent key loss, key recovery

The first factor to consider is the need to change the keys. If you have delegated encryption to an employee, you want their key to become useless if they are no longer trusted. So you switch to a new key, encrypting future data with it.

But this raises a problem: What becomes of the old data? There are two possibilities: Either the old data continues to use the old key, or it is updated to use the new key. The second, though obviously preferable, is technically extremely difficult to achieve. Updating old data on disk requires re-reading and encrypting it with the new key – a time-consuming process. Re-encrypting data on tape, especially off-site tape, is more challenging still. All old tapes would have to be recalled and rewritten.

If data is not re-encrypted, the question becomes one of how to deal with data encrypted with two different keys. If all new data uses the new key, and all old data uses the old, you will have to switch between keys based on the data set being read. Some applications may be able to handle this switch better than others. In fact, some applications cannot handle switching at all, effectively destroying all old data when the key is switched.

The question of changing keys, and the possibility of data loss, raises another consideration: protecting keys. It is essential that the right key is available to read any data set in the future. No matter how well your application deals with old and new keys, no application will be able to read encrypted data without a valid key.

One best practice for encryption keys is known as key escrow. This service, normally provided by a trusted third-party, holds keys off-site in non-volatile media. Key escrow is akin to entrusting a lawyer with a document, or locking a key in a safe deposit box. It ensures that your key will be available to you in the future and available within a time frame that supports committed RTO (recovery time objective). This is especially critical for disaster recovery preparation, since all on-site resources, including encryption keys, could be lost.

Some modern systems also include specialized key recovery functions. One storage security vendor provides an encryption appliance that allows a quorum of key recovery cards to recover lost keys from their encryption device. In this system, each trusted individual is given a special key recovery card. These cards are useless on their own, but can be used to convince the application that an encryption key is being requested for a valid purpose. While not a full disaster recovery solution, this key recovery technique provides an additional level of protection.

Protocol upgrade

Just as changing keys can make data unreadable, switching from one encryption protocol to another is a challenge. Remember, this is exactly the same problem you already manage as tape technology matures and we move from reel to reel, through DAT, to DLT to SDLT to LTO, etc. As with a change in tape technology, so with encryption technology, either all data must be re-encrypted or a dual-protocol system must be used. The latter is not preferable, however, since the rationale for switching from old protocol still applies to that old data.

Why switch protocols? Weaknesses in encryption protocols are discovered fairly frequently, and older protocols eventually fall out of favor. You may also choose to move from one encryption vendor to another and different vendors support different protocols.

Therefore, a procedure must be developed for a protocol switch. This is a time-consuming process, requiring a great deal of personnel and technical resources. All online and near-line data must be re-encrypted, and all offline data (backup tapes, DR copies, and archives) must be recalled. Some vendors provide protocol upgrade tools, but these merely assist in the mechanical re-encryption procedure, not the overhead of implementing this process.

Preparing for loss of your encryption vendor

One of the biggest crises for encryption users would be the loss of the vendor of their encryption technology. Although it would presumably still function after the vendor shut their doors or cancelled the product, it would be foolish to continue using it.

For this reason, the loss of an encryption vendor should be considered similarly to a protocol upgrade. That is, all old data should be recalled and re-encrypted with a new scheme. The large cost of this move should be considered when evaluating products. Which vendor is most likely to continue supporting their product, even if it is no longer current? Some vendors might even be willing to post a bond or place their software code in escrow to protect against this scenario.

SUMMARY

Implementing secure data protection strategy requires planning and preparation. Getting started begins with developing the strategic policies concerning what data needs to be protected and then identifying that data and any copies of it within the enterprise storage environment.

The next step is selecting the most secure method for protecting the most critical data. This could mean electronic vaulting or data encryption. When it comes to encryption, the type and quantity of data to be encrypted, the capabilities of the existing reference architecture, constraints imposed by time windows, physical logistics, and RTO requirements must all be considered. This is true for electronic vaulting as well. For environments where limited amounts of data are to be encrypted, then application/database encryption or backup application-level encryption may be appropriate. It also may be appropriate to vault this data electronically. For encryption of large amounts of data on selected hosts, file system encryption might be a good choice. For wide-scale encryption needs, a network-based encryption appliance would be the most likely choice.

With any approach, the management process around secure data protection needs to be addressed. This includes good encryption key management. The key needs to be totally secured yet readily available in time of need, and readily returned after the need has passed. Some of the appliances provide assistance in this area, making them even more attractive. Operating system vendors provide guidance in this process as well.

The standard operating procedures (SOPs) governing security of data at rest must contain a metrics base that tracks not only completion and compliance, but also the logistics management of both the physical data container and most importantly, the encryption key itself.

Finally, everyone who manages, administers, or operates IT infrastructure needs to become fully security conscious. Data protection security is as much a culture of awareness as it is a corporate policy directive. To truly protect the organization's critical data, continuous focus on culture, practice, and control is imperative to a successful, secure data protection strategy.

MYTHS, REALITIES AND ADVICE ON SECURE DATA PROTECTION

While security may be in the headlines, it is one of the least understood areas of IT. This lack of knowledge has manifested itself in a series of myths about data security and backup encryption:

Myth: It is the responsibility of the backup administrator to worry about the integrity of backup data.

Reality: Backup data integrity and security are the responsibility of everyone in the company who is responsible for information protection and security.

Advice: Every company should have a Chief Risk Officer (CRO), a Chief Information Security Officer (CISO) or General Counsel representative that can communicate the importance of protecting corporate assets and someone who can follow the process of information security and protection.

Myth: The backup process is secure.

Reality: Think this through. IT employees generally do backups late at night. The tapes are often stored in unmarked boxes, picked up by delivery services, and transported over public transportation infrastructure. Even if nothing malicious occurs, tapes get lost, people make mistakes, and equipment fails. Just one lost tape could have devastating consequences.

Advice: Given these details, it is best to assume that the backup process is insecure and live with this risk or address it directly through tape encryption.

Myth: Hackers use networks like the Internet to get into systems; they do not steal backup tapes.

Reality: The ICI example at the beginning of this paper, plus other recent examples, negates this misconception. Data thieves are no different from other criminals in that they look for the easiest way to commit their crimes and get away with it. Unprotected tapes that can be easily stolen present a very attractive target.

Advice: Encrypt the most sensitive customer data in your environment that you back up. If there is a way to steal something, "data thieves" will figure out a way to get it.

Myth: Encryption is slow and expensive.

Reality: This used to be true, but abundant and cheap processing power is now readily available. Specialized manufacturers sell lightning fast encryption chips, and these chips are often integrated into encryption solutions that encrypt at "wire speed." Tape encryption is a modest insurance investment that won't impact the backup window.

Advice: Do not be afraid to explore multiple options for encrypting data. Utilizing encryption from the backup software is not always the answer.

Myth: Encryption is the IT equivalent of “rocket science” and remains the domain of the digital elite.

Reality: Encryption is now a mainstream technology. The most common example of encryption is the SSL/TLS protocol that secures web transactions. If you see HTTPS in your browser window or a lock icon at the bottom of a web page, all communications use SSL/TLS and are therefore encrypted. Many companies also utilize VPNs for remote user access. This too performs encryption functions. Encryption is simply a standard and prolific way to secure data.

Advice: Leverage the knowledge inside the company as it pertains to encryption and how it is used today. Chances are that help is closer than you might think. Seek help from service providers and security experts.

Myth: Backup encryption is ineffective. Hackers can simply “crack” the tapes.

Reality: This false impression has its roots in reality. Many backup servers provide encryption using the 56-bit Data Encryption Standard (DES), which became a National Institute of Standards and Technologies (NIST) standard in 1976. DES was in fact “cracked” by researchers in 1998 because its 56-bit encryption keys could be discovered through “brute force” by high-powered computers. Today’s tape encryption products no longer use 56-bit DES but rather much stronger encryption algorithms like 128-bit 3DES (“triple DES”) or 256-bit AES. It would take millions of years to “crack” these algorithms even if you employed the world’s most powerful supercomputers to do it.

Advice: Utilize the latest and greatest in encryption technology. The process of continual upgrades might not be simple, so have a process for doing so. Keep in mind the standards are upgraded for a reason and it makes sense to stay on top of the latest technology available.

Myth: If I do encrypt my backup tapes, I am protected.

Reality: Security is a process, not a product so it is important to look at ALL the risks and threats. For example, do system passwords adhere to a secure model? Are they changed regularly? Do unauthorized personnel have “root” access to critical systems? How are the files unencrypted and by whom? Encrypting the backup tapes provides excellent data protection but it is only a piece of an entire data security plan.

Advice: Having a good process in place for secure backup encryption is paramount to having a good, secure backup strategy. Assess risks, implement controls and technologies, remediate gaps, audit, and review.

Myth: If I am going to do encryption, I must encrypt all my data.

Reality: It is not necessary to encrypt all of the data that is backed up in an environment.

Advice: It is an important part of the job of the CRO or CISO to analyze the data within the corporation that, if it was compromised, could affect the business. This would be the most important information to encrypt.