IRON MOUNTAIN®

OFFSITE DATA PROTECTION

FIVE BEST PRACTICES FOR PROTECTING BACKUP DATA

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 organisations. 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:

01 Assign accountability, responsibility and authority

02 Assess risk

03 Develop a data protection process

04 Communicate the process

05 Execute and test the process

01 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. Integrating storage and backup security measures will help build defense-in-depth protection.

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

90%

of companies suffering significant data loss go out of business within two years.

SOURCE: LONDON CHAMBER OF COMMERCE

02 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, organisations 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, as well as the impact of encryption on recovery time. 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 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 that provide 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.

03 DEVELOP AN INFORMATION PROTECTION PROGRAMME

ADOPT A MULTI-LAYERED SECURITY APPROACH

Adopt a multi-layered approach to data protection by applying best practices for the data network 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.
- **AUTHORISATION** Enforce privileges based on roles and responsibilities rather than 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. 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 method 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, making it difficult to duplicate the data in a timely fashion. There are various methods of addressing this issue. The first method starts with optimising the backup system to decrease the amount of time it takes to complete the original backup. Then, multiple high-speed tape drives can be used to create the second copy for off-site purposes. Another way 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 saves the time needed to 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 off-site 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 used to access the off-site storage should be analysed for security practices. Media should be placed in locked containers before leaving the data centre and subsequent tracking done at the "container" level. Tracking should be performed by scanning bar codes every time a tape container is moved, including at data centres and at off-site locations. Media containers 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. Data destruction can be performed on-site with the proper degaussing equipment, or via a third-party service. (If performing data destruction on-site, ensure that degaussing equipment is rated for the correct media.) Data destruction is best performed via an organisation that provides a certificate of destruction.

UNDERSTAND YOUR DATA'S CHAIN OF CUSTODY PROCESS

Another critical element in secure media handling is to ensure that off-site storage vendors follow best practices. Here is a baseline of things to consider:

- **ON-SITE VULNERABILITY** Do not leave tapes in an unlocked container like an open cardboard box at the reception desk to await pickup. Pickup should follow 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** When a company stores your critical data, you must be certain it conducts background checks on every one of its employees.
- **THE COMPANY SHOULD HAVE A COMPLETE CHAIN-OF-CUSTODY PROCESS** Talk to the off-site storage vendor about the entire process of how media is handled from start to finish. Look for an emphasis on physical

security, along with audit and control mechanisms to ensure that the process is being followed. It is inadvisable to move sensitive data in a vehicle emblazoned with the vendor's name, easily identifying it as carrying sensitive data.

- **CONTAINER VAULTING** Container vaulting tracks tubs or boxes, but not their contents. Most off-site storage vendors support this type of vaulting.
- **PHYSICAL SECURITY CONTROLS** Facilities should be appropriately secured. No unauthorised person should be able to gain access to the vaults.
- **ENVIRONMENTAL CONTROLS** Tapes and other media should never be stored in a vehicle's trunk, or any other non-environmentally controlled location. For tape storage, the environment must be strictly controlled, including temperature, humidity and static control. Dust is the enemy of most media and media recording devices. 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 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 vaulting data electronically and bypassing the need to transport 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. Data can be encrypted and moved via the Internet to a secure backup data facility. Electronic vaulting may not be a practical solution for all company data, but it may be practical for data that is distributed on file servers or personal computers. Distributed data can represent 60% of a company's information and is difficult for IT to control.

Make sure that the vendor offering these services encrypts data while being transferred and when it is at rest. 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.

When a company stores your critical data, you must be certain it conducts background checks on every one of its employees.

04 COMMUNICATE THE PROCESSES AROUND INFORMATION PROTECTION AND SECURITY

Now that the process has been defined for ensuring that sensitive data is properly protected and handled, it is important to ensure that the people responsible for carrying out its security are informed and trained. Security policies are the most important aspect of assigning 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." Organisations 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 – pointing to a real payback for doing the security "grunt work."

05 EXECUTE AND TEST THE INFORMATION PROTECTION SECURITY PLAN

Secure data protection is not about technology; it is about process. That is why it is important to test the process. 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 are in place that need to be deployed for information classification.

Test the process once it is in place. Remember, the test 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 staff who may be less familiar with the process. This testing 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.

It takes **19 days**
to re-type 20Mb
of lost data.

SOURCE: REALTY TIMES

Every **15 seconds**
a hard drive crashes.

SOURCE: HARRIS INTERACTIVE

2000 laptops
are stolen or lost
every day.

SOURCE: HARRIS INTERACTIVE

INFORMATION HAS A LIFE OF ITS OWN, WE'RE TO HELP AT EVERY STAGE

We can help you take care of your information at every stage of its life, cut costs and improve efficiencies.

ANALYSE AND ADVISE

STORE AND PROTECT

SCAN AND DIGITISE

FLEXIBLE ACCESS

SECURE DESTRUCTION

A PARTNER YOU CAN TRUST

Whatever your size or business sector, we offer specialist service built on these key principles:

TRUST

For nearly 60 years, we have been the trusted partner of companies large and small. We operate from more than 1000 facilities worldwide.

SECURITY

With our secure facilities, vetted teams and optimised processes, your information is always in safe hands.

EXPERTISE

Our strength and depth of knowledge is embedded within our people, processes and technologies. Understanding compliance challenges enables us to help you get the most from your information assets while reducing costs.

CUSTOMER FOCUS

Our commitment to service excellence gives you 24-hour support every day.

SUSTAINABILITY

By helping you reduce the information you need to keep, and recycling what you don't, we can help you fulfil your own sustainability commitments.

CONTACT US TODAY

For more information and advice on how Iron Mountain can help with your information management, please visit www.ironmountain.co.uk or call 0800 270 270.

IRON MOUNTAIN®

UK-OSDP-02-0610-01-EN