
Secure Data Protection: How Effective Is Your Strategy?

Doing it is important. Doing it right is essential.

In today's environment of heightened business risk, safeguarding of data isn't merely an option, it's an urgent necessity. That's why data encryption and backup have become such hot topics in management boardrooms and IT shops. Everyone wants to have a bulletproof data protection program in place.

- A successful program requires careful preparation; a haphazard plan can be almost as bad as no plan at all. "Watch Out for Hidden Traps in Data Protection Planning" can help you avoid seven common mistakes.
- Data thieves are more sophisticated, and their operations more brazen, than ever. Read "Best Practices Can Help You Foil Data Thieves" for some timely tips on safeguarding your sensitive data from the bad guys.
- As the Gershwin song goes, "It ain't necessarily so"—not everything you've seen and heard about safeguarding data is the real deal. "Common Myths About Data Protection" will help you sort fact from fiction.

As the dangers associated with data loss increase with every passing day, there's no better time than right now to ensure that you're taking the right steps to protect your organization's sensitive data. We hope you find the information in this issue of *Business Insights* helpful to your planning efforts.

###

Common Myths About Data Protection

Don't believe these "truths" that flunk the reality test

Just because a lot of people are talking and writing about data protection these days, that doesn't mean everything they say is the truth, the whole truth, and nothing but the truth. The following statements, generally accepted as gospel, simply don't hold water when subjected to closer scrutiny.

Myth #1: The backup administrator is the only one who has to worry about the integrity of backup data. *Fact:* Everyone in the organization who's responsible for data protection and security is responsible for backup data integrity. It is true, however, that one person should be designated to communicate its importance and monitor the process.

Myth #2: Our current backup process is secure. *Fact:* Stuff happens—and it always seems to happen at the worst possible time. Tapes get lost or stolen, people make mistakes, equipment fails. The question isn't *whether* it will happen to you; it's *when* it will happen.

Myth #3: Hackers use the Internet, not backup tapes, to invade systems. *Fact:* Data thieves are like any other thieves—they take the easiest route to their objective. If that means stealing unprotected tapes, then they'll steal unprotected tapes.

Myth #4: Encryption is slow and expensive. *Fact:* Encryption can be fast and cost-effective, thanks to modern cheap, abundant processing power featuring speedy encryption chips and products.

Myth #5: Only those with a doctorate in computer science are able to understand encryption. *Fact:* Encryption has gradually become a mainstream technology—a standard and increasingly accepted method of safeguarding sensitive data.

Myth #6: Backup encryption won't prevent hackers from deciphering tapes. *Fact:* That was actually true some years ago, but not anymore. The latest and greatest data encryption products utilize much stronger encryption algorithms that make it far more difficult to glean information from encrypted tapes.

Myth #7: We're protected if we encrypt our backup tapes. *Fact:* That's only partially true at most. It's crucial to scrutinize *all* potential security risks and threats, not just those addressed by the act of encryption itself. Are passwords themselves secure? Are they changed frequently? Who has access to critical systems? Who encrypts the files and how? Examine the whole process, not just one component of it.

Myth #8: It's necessary to encrypt all of my data. *Fact:* The only data that should be encrypted is business-critical data—in other words, information that could affect the business if it were to be compromised. (Other articles in this issue of *Business Insights* offer additional information on data encryption.)

At Iron Mountain, we strongly advocate data encryption and urge you to consider its benefits. The best way to proceed is by disregarding the myths and arming yourself with the facts.

###

Watch Out for Hidden Traps in Data Protection Planning

***Make a checklist, avoid some common mistakes,
and keep your data really secure***

The ideal data protection program is one that safeguards centralized and distributed data consistently and automatically, across all business locations, while keeping it highly secure. Achieving these results requires careful preliminary planning to ensure an efficient structure. It's a good idea to begin by going through a checklist of questions that need to be dealt with up front:

- What data is to be backed up?
- How often will it be backed up?
- What storage media will be used?
- Where will backups be stored?
- How will they be identified and retrieved?
- How long is a backup to be retained?
- What will be the disposition of the backup at the end of the retention period?
- Who is authorized to back up and recover data?
- Who will be responsible for the procedure?

Ask yourself if your strategy avoids these common traps:

Trap #1: Not assigning accountability for data protection

It's easy to shrug off the importance of accountability by saying that "everyone in the organization is responsible." That's true as far as it goes; it just doesn't go far enough. Besides establishing strong policies and procedures for all employees to follow, your

plan also needs to identify strategic roles within the organization so that everyone knows who has the accountability, responsibility, and authority for implementing specific data protection tasks.

Trap #2: Not providing adequate IT resources

Many organizations are struggling to achieve profitability, or even just stay afloat, by keeping a tight rein on expenses. At the same time, they're trying to cope with ever-increasing data backup and storage requirements. Something has to give, and all too often it's IT, asked to carry out its mission with smaller budgets and fewer people. But that's foolish economy; how can IT be expected to administer an effective data protection program without an adequate budget and headcount?

Trap #3: Not applying consistent backup practices beyond the boundaries of corporate headquarters

While it's obviously essential to protect the data at corporate headquarters, the enterprise is far-flung, extending to mobile users, remote locations, and branch offices as well. A good data protection plan requires consistent, uniform backup practices across the enterprise rather than settling for patchwork approaches that vary from place to place.

Trap #4: Not being prepared for regulatory compliance, virus strikes, and malicious behavior

Just backing up data isn't enough. In today's business climate, "it's always something." Companies must always be ready to access data in order to comply with increasingly burdensome regulations, and to rapidly restore data after a virus attack or hacking intrusion. The ability to anticipate these unwelcome occurrences is an essential component of any data protection program.

Trap #5: Not being able to comply with the business mandate for near-zero data loss and downtime

A disaster recovery plan includes metrics for how much lost data and downtime the organization can tolerate. If these figures are near zero, there isn't much margin for error. Is IT fully prepared to carry out prompt, effective disaster recovery? If not, either the metrics should be revisited or the IT department provided with enough resources to ensure compliance with the metrics currently in place.

Trap #6: Not setting up a method for handling and storing encrypted data

Where it should be the last line of defense, tape encryption is sadly neglected in many data protection plans. It's true that encryption used to be a slow, expensive process—but with today's cheap, abundant processing power and blazing-fast chips, it has become a mainstream technology. Although it's not necessary to encrypt all backed-up data, provisions for the handling and storing of encrypted data should be an integral component of any plan.

Trap #7: Not scheduling regular monitoring and updating

It's dangerous to assume that even a well-designed data protection program is going to roll along forever like some kind of perpetual motion machine. On the contrary, it should be regularly monitored and updated to keep pace with ever-changing technical and business requirements.

By anticipating these traps and planning around them, you're on the road to success in creating an effective program to keep your precious data safe and secure.

###

Data Encryption: Choose Your Methodology

You can encrypt at database, OS, network, or backup software level

You've performed a thorough cost/benefit analysis on backup data encryption. You've concluded that encryption of your sensitive information is a good idea. Next question: How should you go about doing this? A number of methodologies are available:

- **Application/database encryption:** Highly confidential data such as credit card numbers, employee salary information, and personal medical data are often encrypted at the database level. Database programs include tools for encrypting tables, rows, or columns so that the information can be viewed only by those who are authorized to do so. This method saves time and space by encrypting only the data that needs it. What's more, it encrypts data at its point of origin, adding an extra measure of security.
- **Operating system encryption:** With today's operating systems, it's possible to encrypt data stored inside a file system, directory, or individual file. However, this method does consume a great deal of processing power and can slow down performance, since data must be decrypted before it can be accessed. Another concern is key management, discussed later in this article.
- **Network encryption:** New-generation hardware security modules residing on a SAN or LAN offer high-speed, transparent encryption with minimal latency. These modules have several advantages. First, they're fast. Second, they're versatile because they're available in all kinds of configurations to suit specific requirements. And third, they're less expensive than other methods.
- **Backup application software encryption:** The physical transporting of backup data has significant drawbacks; tapes and other media can be damaged, stolen, or mislaid in transit. Consider *electronic vaulting* instead, particularly for backup of data that's distributed on file servers or PCs—and that's probably some 60 percent of your

organization's data. Iron Mountain specializes in provides electronic vaulting, whereby data is encrypted and moved via the Internet to a secure offsite backup facility. Your precious information is then readily available for disaster recovery or litigation support.

So why isn't encryption more widespread?

If data encryption offers so many benefits, you may wonder why isn't it a more widespread practice. There are several reasons:

- The process of performing host-based encryption can slow down, and interfere with, critical business operations.
- The process can slow the rate of data being transmitted to the host and subsequently to the backup medium.
- Encryption makes files harder to compress, requiring more backup tape and adversely affecting performance.
- The other half of encryption is, of course, decryption. Decryption calls for keys, without which all encrypted data is useless. Accordingly, the encryption process can't work properly without adherence to a set of management best practices for changing keys when necessary, preventing key loss, and recovering keys.

Despite these drawbacks, more and more large organizations are either already encrypting, or at least considering, encrypting their sensitive data. In today's world, they just can't afford to leave it vulnerable to a potential invasion of hostile eyes.

###

Best Practices Can Help You Foil Data Thieves

Build your information protection plan around five fundamental steps

Willie Sutton was once asked why he persisted in robbing banks even though he was invariably caught and sent to prison. His answer was short, sweet, and sensible: “Because that’s where the money is.”

Modern-day Suttons are more likely to rob business data—and why not? It’s easy to get at. There’s lots of money to be made. Almost anyone can do it. And there’s no need to bother with guns, ski masks, and getaway cars.

It seems strange that, even though most large organizations are fully aware of this growing threat and have taken measures to keep their data secure, it still isn’t. There are several reasons:

- IT continues to focus on traditional firewalls and gateway appliances to protect the network perimeter. Meanwhile, new threats bypass perimeter defenses to attack business-critical systems and confidential data.
- Many organizations aren’t paying enough attention to the vulnerable storage infrastructure that contains business-critical data. An inside attack might have serious consequences, among them compliance problems, intellectual property theft, and data corruption.
- It’s all very well to back up data regularly and maintain offsite copies, but six out of ten organizations don’t encrypt their backup tapes—an open invitation to data thievery.

In short, organizations need to address not just host system security but data security across the entire enterprise. Toward this end, intelligent storage practices should be part and parcel of an overall best-practices strategy built on *assigning, assessing,*

developing, communicating, and executing and testing:

- **Assign accountability, responsibility, and authority.** Make storage security a function of overall information security policies and architecture. Even if your storage team is responsible for backup and storage, it's wise to integrate those areas of security with the employees who secure the rest of the infrastructure. That establishes a second line of defense.
- **Assess storage risk as it pertains to information security.** Examine every step of your backup methodology to uncover security vulnerabilities. Establish a chain of custody for the handling, supervision, and control of storage media. If a risk analysis exposes numerous vulnerabilities, strongly consider encryption of all data that contains sensitive information. (Refer to other articles in this issue of *Business Insights* for more about encryption.)
- **Develop an information protection program that ensures the safety of your organization's data, wherever it may be.** Apply the best practices of your data network to your storage network and add in layers of authentication, authorization, encryption, and auditing. Copy your backup tapes to allow for long-term environmental or physical damage of the originals. Monitor your offsite storage vendor to ensure his compliance with your best practices.
- **Communicate the processes for information protection and security.** Warn your business managers of the risks, costs, and countermeasures that can be expected with your program. Make sure your staff are properly trained and understand the benefits of the program; they'll be more likely to be vigilant in ensuring that it's properly executed.
- **Execute and test the plan.** Once the end-to-end plan has been developed, make sure that the proper tools, technologies, and methodologies are in place. Test the process, both backup and recovery. Keep in mind such conceivable scenarios as server or tape loss, network failure or intrusion, and others that might adversely

affect business operation.

Remember that old TV show *The A-Team*? When, at the end of an episode, the team triumphed over the bad guys, Hannibal Smith would light a cigar, rub his hands together, grin contentedly, and announce, “I love it when a plan comes together.” You too will love it when your information protection plan comes together—and it surely will if you follow these fundamental steps. Don’t let the bad guys win!

###