Make the Right Choice

Michael R. Baldani
Product Marketing Manager, NA Marketing
Iron Mountain
michael_baldani@ironmountain..com

As Data Protection and Recovery grows in business importance, companies are turning to trusted outsourcers like Iron Mountain to ensure their data is protected and available

As news of online fraud and data breaches hit the headlines, the issue of data protection has moved out of the data center and into the executive suite. The reason is simple: these days, how well a company protects and recovers its data could directly affect the bottom line. According to the *Wall Street Journal*, data breaches can cut about 1 percent from the stock price of affected companies.[1] But building a data protection strategy has grown in complexity as well as importance, and several trends highlight the new challenges that many Senior IT Managers face. Companies increasingly rely on technology to store and analyze vital business data, from customer contact information to financial records to intellectual property. That increased reliance can also result in vulnerability, as data losses that aren't quickly recovered can have disastrous business consequences. Alarmingly, much of that data has also moved from the safety of a centralized data center to less secure devices, such as remote servers in regional offices or the laptops of mobile workers that are not regularly backed up. Moreover, the increase in government regulations that mandate how companies store, archive and secure particular types of data further deepens the challenges of data protection.

These business trends should drive a wholesale change in how business data is protected and recovered. Instead of building a disaster recovery plan centered only around the data center, companies must also ensure that distributed data—on laptops, PCs and remote office servers—can be quickly and reliably recovered. These plans must also factor in the stringent security and recoverability mandated by the new regulatory climate. The bottom line: business owners and technology people must rethink the way they protect and recover corporate data.

"The changes in the business world are reflected in the new approach that companies are taking to data protection," says Curtis Preston, vice president of data protection at GlassHouse Technologies in Framingham, Mass. "Instead of just backup, data protection must encompass backup, disaster recovery as well as storage, security and archiving."

The answer is to build a strategy that both protects and recovers data. An effective data protection and recovery strategy not only restores data that has been destroyed, damaged, or misplaced but also prevents data from falling into the wrong hands as well as ensures that companies are in compliance with regulations affecting their industries.

"Businesses need a data protection plan that incorporates all corporate data, from the server to the laptop," says Brian Babineau, an analyst at Enterprise Strategy Group in

Milford, Mass. “And as regulatory compliance comes into play, we’re seeing a convergence of data protection and security — you can’t just protect it by backing it up. You need to secure it so that if it falls into the wrong hands, it can’t be misused.”

The key for any organization – regardless of its size or the industry in which it plays – is to implement a data protection and recovery strategy that mitigates business risks, reduces costs, increases compliance and helps improve overall business service levels. Doing so involves performing a multivariate cost-benefit analysis with the business managers and the technology team which assesses the value of business data with the costs of downtime.

Faced with both a high opportunity for failure and great deal of risk, many companies are choosing outsourced managed data protection as the fastest, safest road to ensuring that data is consistently protected, secured, compliant and – most importantly – quickly recoverable. With such high stakes — many companies live and die on their ability to access and use data 24/7 — choosing the right partner is a vital decision. Some of the things that should be evaluated include the following:

- **Reputation.** Trust is paramount in a relationship where so much is at risk, so look for vendors with an excellent reputation and *proven* track record of helping companies successfully recover their data during regional or national disasters.

- **High Accessibility.** Enterprises need the ability to restore data themselves, regardless of whether it’s in the data center, on a PC or a remote server. Electronic Vaulting, for example, offers a secure Web interface that allows IT administrators to easily and quickly restore lost data themselves, a valuable commodity in an increasingly mobile world. Online access also allows companies to access and manage media, control authorization levels, declare a disaster and make media requests. “Self service requirements are part of the consumer environment today,” says Babineau. “They want the ability to get people involved, but they want the ability to do it on their own when they want.”

- **Menu of services.** As data protection and recovery increases in scope, so too must the services that data protection vendors offer. These providers should offer services that complement each other for a complete data protection and recovery strategy. Look for the ability to back up and recover both centralized and distributed data, as well as encryption and digital archiving.

- **Distributed Data Protection Services**. With critical data increasingly stored on decentralized sources such as remote servers or laptops, data protection vendors must offer a complete strategy to protect that data. Electronic Vaulting offers services to protect data that resides outside the

data center, automatically and consistently, which not only ensures backups are being done to set policies, but also ensure recoverability.

- **Service Level Agreements.** Vendors should be able to tailor SLAs to protection and recovery priorities of each customer, and offer a technology solution that supports each SLA level. Tape is an inexpensive solution for low priority data, for example. Electronic Vaulting, which backs up data online and offers on-demand recovery, provides easily manageable data protection with recovery points and recovery times that range from a few minutes to 24 hours, depending on service level requirements.

- **Top Equipment.** Conduct due diligence to make sure that the vendor's infrastructure is everything you'd want. With electronic vaulting, look for encryption and a fully manned service operations center to monitor and manage services. With backup tape storage, look for premium data centers, vault facilities with top-line security, gaseous fire suppression systems, backup generators, and tight controls around temperature, humidity and static electricity.

- **Security.** Security covers two realms — the physical security needed for facilities, personnel and media transportation, as well as encryption technologies for safeguarding sensitive data in transit, either through electronic vaulting and on backup media. "There should be reasonable repeatable processes in place to make sure that only the right people have access," says Babineau.

- **Consistent, secure processes** for handling and transporting media from start to finish that prove chain of custody. "Look for vendors that properly handle and store tapes, from bar-code scanning for chain of custody control, to the ability to electronically inventory the vaulted media," says Preston.

In the final analysis, implementing a comprehensive data protection and recovery plan requires an ongoing strategy rather than a one-off program. When the stakes are nothing less than business survival, data protection becomes a vital business issue--and using trusted experts to safeguard this asset becomes the most viable solution. By implementing a data protection strategy which includes choosing the right partner for data protection and recovery, CIOs ensure that business leaders can depend on the continuing availability and integrity of the data engine that drives their organization.

Call to action: For more information on how to implement data protection and ensure recovery, check out www.ironmountain.com. Or call Iron Mountain at 800-899-IRON.

Footnotes
1. June 15, 2005 Wall Street Journal