

Spotlight on a **complete** data protection strategy

As more companies depend on online sources of information to do business, protecting data across the enterprise is increasingly in the spotlight. Building a robust data protection strategy, then, is now a business requirement. **Kevin Roden**, CIO of Iron Mountain, shares his perspective on best practices with data protection.

What are some of the issues driving this new focus on data protection?

RODEN: For one, the mobility of the workforce is leading more critical information beyond the protection of the data center. Some research indicates that as much as 60 percent of business data is maintained outside of the raised-floor environment. Moreover, we now live in a world with “anywhere access,” where secured resources are utilized from public networks—VPN via the Internet, for example. The trouble is, we don’t know where our employees are communicating from. They could be sitting in a coffee shop, with the competition looking on. This lack of certainty increases the chance that sensitive information could be compromised.

The other thing has to do with the regulatory environment and public awareness. Based on some high-profile incidents involving corporate corruption

and stolen personal information, the federal government has reacted by instituting regulations that mandate the protection of sensitive data. Additionally, state legislation requires companies to disclose instances of stolen private information. As a result, enterprises are now trying very hard to stay on the safe side in terms of disclosure. And companies are realizing that they should be taking appropriate measures to protect all backup data.

Why have information security breaches become so pervasive?

RODEN: Stealing sensitive information such as customer data is highly lucrative—at 10 cents per piece, 5 million credit-card numbers turns into \$500,000. The other reason is that as companies rush to bolster productivity, they roll out technology quickly, and they sometimes neglect to build security into the design. As a result, security measures are bolted on as an afterthought, and can leave some vulnerability in situations where confidential data is an easy mark. In my opinion, breaches are becoming public knowledge more often than they were 5 years ago. There is also more interest in the press, and the public understands the importance of private information more than ever. So it’s not that there are more

“In an age where technology downtime can significantly affect corporate revenue, it is critical to proactively protect against data loss,” said Rich Miller, vice president and chief information officer for Cerner. “Iron Mountain’s PC backup service is a key component of our information lifecycle management strategy for distributed data. The benefits of using the subscription service have been recognized at all levels of our company, particularly by associates who have used it to recover from a lost, stolen or destroyed device.”

breaches so much as it is that the ones that occur are more public.

With all that risk, it sounds as if companies need to find a way to assign accountability for data protection.

RODEN: “Every employee is responsible” is the short answer, but it’s really a matter of creating and enforcing strong policies and procedures. People in our company get an information packet that contains all of the policies and procedures that deal with data security as well as data protection. This includes the use of tools and passwords. It’s also important to make sure that security of backup data is a component of your firm’s overall information security policies and procedures. Be sure to identify roles within the organization so people know who is responsible for doing specific tasks within the data protection strategy.



Kevin Roden, CIO of Iron Mountain

Make sure you are providing the right level of protection for each specific data set

What are the main components of a companywide data protection approach?

RODEN: The first is organization. Here, you need to understand the overall scope of the plan, and then define the roles and responsibilities from an organizational standpoint—do we have the right people doing the right jobs? Once you do that, conduct a data assessment—find out where all the data resides between the data center and any remote distributed data, and identify the critical and sensitive information. With this, you need to do a cost benefit—and risk—analysis to make sure you’re providing the right level of protection for each specific data set. Then, development—creates a standard set of program guidelines that include a multi-layered approach, chain-of-custody, and getting all the data under the appropriate levels of protection. Keep in mind this is not a “one size fits all” approach. Once that is done, it’s time to implement the plan based on the guidelines, as well as training staff and conducting internal communications. And finally, you have to go back and test the plan through auditing, and keep in mind that even the best data protection plan should evolve to meet changing technical and business requirements.

What is the difference between centralized and distributed data, and how do you best protect these different data types?

RODEN: Centralized data consists of information at a company’s data center, which is where the primary storage servers and tape management system reside. Distributed data is all of the information stored outside of the centralized corporate repositories. Examples of this kind of data are desktop and laptop PC data storage, file servers in remote or branch offices, and the vast amount of data distributed in local archives on individual PCs. With centralized data, it’s best to first make copies of the backup data and take those copies off-site. Ideally, an experienced, neutral third-party vendor should be chosen to get the critical backup data off-site, off-line, and out of reach, so it is fully protected. Backup media should never be stored in any non-environmentally controlled areas. Rather, it must be protected in state-of-the-art, climate-controlled

vaulting facilities manned by rigorously screened and trained employees to ensure consistent processes and stringent controls for safe data handling. Additionally, a complete chain-of-custody process using bar coding should be demonstrated to ensure tracking of media both on-site and off-site.

When protecting distributed data, it’s critical that all backup processes happen automatically. Once set up by administrators, the data on remote servers, as well as desktop and laptop PCs, should be regularly and automatically captured, encrypted, and transmitted safely off-site. This approach removes much of the backup burden from IT staff while keeping backup data stores current and secure in the event of disaster, large or small.

The Seven Myths of Data Protection

Myth # 1 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.

Myth # 2 The backup process is secure.

Reality: Even if nothing malicious occurs, backup data sometimes gets lost, people make mistakes, and equipment fails.

Myth # 3 Hackers use networks like the Internet to get into systems; they do not steal backup tapes.

Reality: Data thieves are no different from other criminals, in that they look for the easiest way to commit crime and get away with it.

Myth # 4 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.”

Myth # 5 Tape encryption 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. Encryption is simply a standard and prolific way to secure data.

Myth # 6 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. Encrypting the backup tapes provides excellent data protection, but it is only a piece of an entire data security plan.

Myth # 7 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.

How do you communicate data protection policies, and disseminate them throughout management?

RODEN: Data loss and information theft are a business issue, not an IT issue. Therefore, an effort to educate executives on risks, threats, and potential losses from data theft should be conducted. Additionally, the education effort should include the costs to defend data against unauthorized access. That way, corporate officers can make informed decisions on cost/benefit profiles for complete backup data protection.

