Data Storage Security

Tom Olzak

February 2006

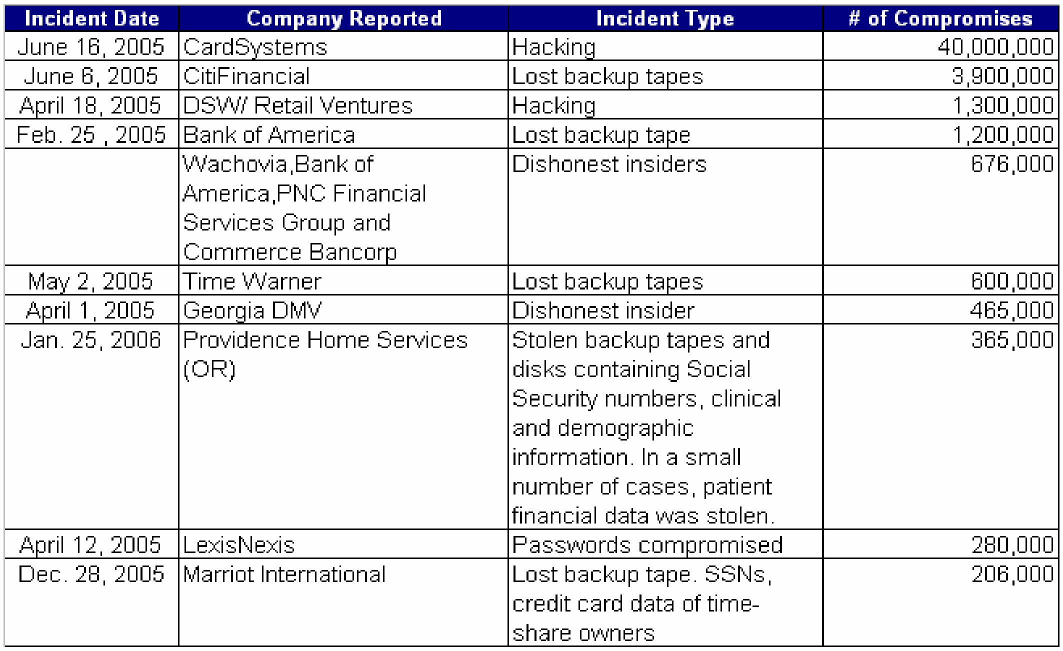
Data in transit, across and between company networks, are usually the focus of extensive security efforts. However, organizations typically regard data residing on internal storage devices as "secure enough." Databases and flat files stored on server drives or on SAN disk arrays don't move outside the security perimeter; so why worry?

In this paper, we'll explore data storage vulnerabilities, the risks these vulnerabilities present to an organization, and ways to effectively manage those risks.

The Challenges

Over the past few years, companies improved the security for information that moves across the Internet and other public connections. But although it's estimated that 80% of all business information is now stored in electronic form (Howarth, 2004), most organizations have done little to protect data stores.

The Privacy Rights Clearing House keeps a list of reported incidents going back to February, 2005. The total number of consumers affected exceeds 52 million. Listed below are the top ten incidents sorted by the number of individuals reported compromised (Privacy Rights Clearing House, 2006):



Incident Date	Company Reported	Incident Type	# of Compromises
June 16, 2005	CardSystems	Hacking	40,000,000
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
April 18, 2005	DSW/ Retail Ventures	Hacking	1,300,000
Feb. 25 , 2005	Bank of America	Lost backup tape	1,200,000
	Wachovia,Bank of America,PNC Financial Services Group and Commerce Bancorp	Dishonest insiders	676,000
May 2, 2005	Time Warner	Lost backup tapes	600,000
April 1, 2005	Georgia DMV	Dishonest insider	465,000
Jan. 25, 2006	Providence Home Services (OR)	Stolen backup tapes and disks containing Social Security numbers, clinical and demographic information. In a small number of cases, patient financial data was stolen.	365,000
April 12, 2005	LexisNexis	Passwords compromised	280,000
Dec. 28, 2005	Marriot International	Lost backup tape. SSNs, credit card data of time-share owners	206,000

Some industry analysts believe that the number of reported events might be less than 20% of the total number. This is due to the reluctance on the part of organizations to report these kinds of incidents to consumers, investors, and regulatory agencies. Note that only two incidents appear to be the result of an external hacker gaining access to the information. The majority of incidents appear to have been caused by employees or tape management services.

Employees are an organization’s greatest asset; they can also be its greatest vulnerability. There are two types of data security incidents employees can cause – intentional and unintentional. Intentional compromises are typically caused by disgruntled employees or those individuals trying to make a little extra cash on the side. Employees who cause unintentional compromises make honest mistakes that might cost a business money, customers, or investors. Using encryption to hide from organizational job roles the information not required for day to day activities is a good way to minimize exposure to employee activities.

One of most common causes of unauthorized release of personal information appears to be lost backup tapes. Most organizations fail to encrypt sensitive information contained on tapes that travel from data centers to off-site storage. With access to the right hardware and software, retrieving consumer information from tape is relatively easy.

There are many ways an external attacker can access credit card numbers, protected health information, passwords, account IDs, banking information, or social security numbers. Because most organizations focus on securing the network perimeter while largely ignoring internal network protection, once an attacker cracks through a firewall or other perimeter device, he can usually take his pick of databases, flat files, or email message stores he would like to browse.

Penalties for not preventing accidental or malicious exposure of sensitive information go beyond fines associated with regulatory constraints like the HIPAA. A business could also experience public and investor loss of confidence leading to business failure. Facing these issues, what can businesses do to protect their customers, employees, and themselves?

The Solution

Encrypting data at rest seems to be one answer. But like all new ideas, it seems to be moving in the direction of "over-kill". Some organizations are encrypting all production data without looking at the value of doing so or at how the encryption process fits into an overall data protection strategy.

Encrypting stored data can be expensive and often intrusive to the way your employees work. Make sure you’re doing it for the right business reasons. And encryption may not be welcomed by all stakeholders. Some of the reasons given by managers and other employees for shying away from encryption solutions include (SPICE, 2005):

- Encryption causes a degradation in performance
- Data might be lost if encryption keys are lost or if disgruntled former employees refuse to provide passwords
- Another password prompt might be added for information access
- Management of encryption systems, including certificates, keys, and passwords, adds addition cost to storage TCO

All these concerns are valid at some level. But security managers must work closely with data owners, database administrators, and network engineers to find the right balance between locking down data and the discomfort or risk the business is willing to accept.

Rich Mogull, a Gartner analyst, documented what he calls the Three Laws of Encryption. These laws are useful guidelines for deciding what to encrypt and when to encrypt it (2005):

Law 1 - Encrypt data that moves

Laptops are great candidates for encryption. Once an attacker gets her hands on a laptop, there are many ways to pull unencrypted data from the hard disk - without knowing the user's password. But, encrypting the information stored on a laptop's drive goes a long way toward strong data protection.

Another storage medium, and one that seems to be in the news more than it should, is the venerable backup tape. Tapes are often misplaced. Even if the information is never compromised, the public disclosure of a tape loss incident can damage an organization.

Email messages are stored in message stores in your mail servers. Like databases, these message stores often contain sensitive information about customers and employees. But information stored in a message store can also include sensitive information about your network - information an attacker can use to dig even deeper into your information assets.

Finally, there are the portable devices. USB storage devices, CD-ROMs, and DVDs can hold a great deal of sensitive information. If one of your users copies employee information to a CD, then leaves the CD unsecured on his desk when he leaves for the night, no level of access control is going to protect that data if found by the wrong person.

Law 2 - Encrypt for separation of duties when access controls aren't granular enough

Application access controls often don't allow the setting of field level permissions. If a user has access to a customer or employee record, she can view all information about that person. Encrypting information in these fields is one way to prevent access outside of a need to know requirement.

Most organizations provide shared folder areas so departments and teams can share information. After all, this is one of the principles upon which networking is built. But denying access to some files or subfolders may be necessary to enforce least privilege - the concept that a user should only have access to data required to perform her daily tasks. Encrypting certain files can enforce another level of access control.

Law 3 - Encrypt when someone tells you to

No matter how well you employ risk management principles to ensure you're making the best use of your security resources, you’ll always have to contend with regulatory constraints. After you've taken a risk-based look at your stored data, take another look to ensure you are protecting your business from the consequences of failing to comply with Federal, State, and Local requirements.

Once you decide what to encrypt, you need to select the right encryption solution. There are many ways to accomplish this. Here are some suggestions:

- For storage area network encryption, consider an inline appliance that encrypts data on its way to storage and decrypts it as it moves from storage to a calling application or user. Appliances add very little overhead to the encryption process. But they don't scale very well for distributed storage environments.
- For distributed environments, agents that reside on the servers or Network Attached Storage devices to be encrypted are a better choice. Centrally managed, the cost of administration can be kept at an acceptable level. A major downside is the potential performance hit your systems may take because encryption and decryption are facilitated in software rather than hardware.
- Consider using the encryption functionality built into operating systems. For example, using the Microsoft Windows Encrypting File System (EFS) is an easy way to allow employees to encrypt folders or individual files. Just be sure to centrally manage the user certificates used for encryption. Using the Microsoft Enterprise Certification Authority is a good way to accomplish this.

But encrypting your stored data should be part of a layered security strategy designed to secure data stored in your enterprise. There is no replacement for traditional physical, administrative and logical access controls. Data storage encryption should just be one weapon in your security arsenal. The following is a list of recommended safeguards, policies, and processes to provide a strong defense for your stored data (Bragg, 2005):

- Ensure applications, network devices, and the network are hardened
- Implement access controls for storage devices
- Provide centralized management for efficient security policy and process implementation throughout the enterprise
- Separate data access from data management; business users of sensitive data should access that data through applications with well designed access controls
- Ensure appropriate physical security for your storage devices and media
- Consider authenticating access between storage devices and from management consoles to storage devices
- Implement monitoring and logging of database access and changes to database security

And as always, make sure user awareness of the importance of safeguarding sensitive information is part of your security program.

Conclusion

It’s the responsibility of every business manager to safeguard the organization’s information. This is accomplished through the development of and compliance to policies, processes, and procedures that specify when and how data are to be protected.

Encryption is one of many safeguards to be considered. It can provide very powerful protection against intentional and unintentional acts. It can also cause increased security management costs, frustration, loss of productivity, and potential loss of critical information. Like all security safeguards, encryption should be deployed judiciously – based on data store risk assessments.

Finally, managers shouldn’t rely on encryption as their only means for protecting information. Rather, encryption should be an integrated part of an overall data storage security program.

Works Cited

Bragg, Roberta (2005, March). *Data at rest is a sitting duck*. Retrieved January 1, 2006 from http://www.redmondmag.com/columns/print.asp?EditorialsID=911

Howarth, Fran (2004, May). *The importance of encrypting data in storage.* Retrieved January 1, 2006 from http://www.it-analysis.com/technology/security/content.php?cid=7074

Mogull, Rich (2005, August). *Management update: use the three laws of encryption to properly protect data (Gartner Research Article G00130839)*. Retrieved February 4, 2006 from http://www.gartner.com

Privacy Rights Clearing House (2006, January). *A chronology of data breaches reported since the ChoicePoint incident.* Retrieved February 4, 2006 from http://www.privacyrights.org/ar/ChronDataBreaches.htm

SPICE (2005, December). *Encryption for data at rest.* Retrieved February 4, 2006 from http://security.health.ufl.edu/eduguides/index.shtml