
How Encryption Supports Compliance

by Rebecca Herold, CISSP, CISM, CISA, FLMI

Encryption is an underutilized security tool. Facing the infinite number of today's risks, threats, and vulnerabilities, encryption can effectively keep unauthorized individuals and systems from accessing sensitive information and thwart many types of attacks. In today's business environment—with sensitive information being stored in multiple locations, many of them mobile—encrypting information is an effective privacy safeguard organizations can add to their arsenal of protection tools.

According to the December 2005 Congressional Research Service (CRS) report from the United States Library of Congress, in 2005, a stolen computer (desktop, laptop, or hard drive) was the cause of a security breach 20 percent of the time. If the information on these devices had been strongly encrypted, the theft would not have been thwarted, but information compromise could have been prevented if someone who did not have the decryption key stole the device.

Consider the growing numbers of electronic storage media and computing devices that are being retired from business use:

According to Gartner, United States homes and businesses combined discard 133,000 PCs each day.

The United States Environmental Protection Agency (EPA) reports that U.S. residents throw away 2 million tons of tech trash each year.

How many of these devices still have sensitive information stored on them when they are discarded? How many organizations remove the data from retired computing devices before trying to recoup some investment by auctioning or donating to charities? Does your organization completely remove sensitive information from retired computing devices?

Careless disposal of confidential information is posing greater problems for individuals and businesses and can result in identify theft, fraud, and legal noncompliance. Increasing numbers of laws and regulations require businesses to follow a standard of due care to protect personal information from unauthorized exposure. Such incidents involving stolen, lost, or purposefully sold storage media containing clear-text data is easily preventable through the use of encryption.

Safeguard for the Unknown

No organization can completely defend against all threats. The number of potential risks and threats is infinite—new ones emerge every day, and many (if not most) are unknown or unanticipated. The incidents resulting from unknowns are typically the events that wreak the most havoc on organizations.

Organizations must implement appropriate safeguards to protect against threats and demonstrate due diligence. One of the best ways to protect information—particularly personally identifiable information that is covered by multiple laws and regulations—from unknowns is to make the information incomprehensible and unusable to unauthorized individuals by encrypting it. Organizations must expect that one of those infinitely unknown threats will result in an incident sooner or later. Strongly encrypting sensitive data will significantly lessen, and possibly eliminate, the negative business impact when a security incident happens.

The Need for Encryption

The porous network perimeter; the growing number of mobile, small, and huge-capacity storage device types; and the numerous ways that data can be sent within milliseconds to multiple locations throughout the world has generated an increasing need to protect information by using encryption. Organizations replace computing hardware more frequently than ever because of how quickly technology is evolving; they subsequently resell the retired equipment in an effort to get some return on their investment. Contributing to these compelling technology factors is the exponentially increasing number of regulatory requirements that necessitate that organizations implement safeguards to protect data more effectively than has been demonstrated in the past.

It seems incidents involving personal information are reported almost every day. Just a few of the many reported incidents that have occurred recently include:

Reported March 4, 2006 in the Vancouver Sun—In mid-2005, the government of British Columbia sold 41 high-capacity data tapes containing clear-text personal information, including sensitive health information and medical notes about at least 65,000 individuals, for \$300 at auction.

Reported March 2, 2006 on CBS4 Denver—A Metropolitan State College of Denver laptop containing the clear-text names and Social Security numbers of 93,000 current and former students was stolen in late February from the home of an employee authorized to take the computer home.

Reported February 24, 2006 by the IDG News Service—On December 15, 2005, a Deloitte and Touche auditor left a backup CD on a plane. The CD contained clear-text names, Social Security numbers, and information about stock holdings held by more than 9000 of McAfee's current and former employees.

Reported December 25, 2005 in Iowa's Des Moines Register—Three-thousand Iowa State University (ISU) employees may have had their personal data viewed by hackers who gained access to two computers earlier in December. One computer held about 2500 encrypted credit card numbers of athletic department donors. The second computer contained clear-text Social Security numbers for more than 3000 ISU employees. The intruder could not read the credit card numbers because they were encrypted; however, the Social Security numbers are at risk of being inappropriately used.



Although encryption will not protect data from all kinds of incidents, such as when authorized insiders abuse or misuse their privileges, it does provide effective protection by ensuring only authorized users with valid decryption credentials can see the data.

Encryption keeps inappropriate viewing and use from occurring when data is lost, stolen, sold, or otherwise compromised. Just consider the June 2005 Citigroup incident in which a backup tape containing information about 3.9 million individuals was lost by UPS while in transit. If the information had been encrypted, the incident would have had much less, possibly negligible, negative business impact to Citigroup and would have presented significantly less risk to the individuals whose information was on the tape.

Encryption Is Not Yet Widely Used

Unfortunately, many organizations still think current encryption solutions are too complex to realistically implement enterprise-wide or have too much negative impact on application and network response times. In August 2005, Forrester Research reported that only 16 percent of North American companies implement data-at-rest (storage) encryption for their databases, and only 48 percent implement data-in-motion (network) encryption to support critical applications. It will be interesting to see how encryption practices change throughout 2006.

Encryption solutions have advanced greatly in recent years. They are now easier to use, easier to implement, are more transparent to the end users, and are comparatively more economical than past encryption solutions.

Legal Implications for Encryption

Organizations, typically at the direction of their legal counsel, will often only implement safeguards such as encryption if explicitly required by the law. For example, in the December 2005 ISU privacy breach, the fact that credit card numbers were encrypted on one system and the Social Security numbers were not encrypted on another system strongly implies that the organization was doing only what was required by the “letter of the law” or the “letter of the contract” rather than implementing a wider interpretation of what is right according to the spirit of the law or performing due care activities to protect sensitive information. Although this theory has not been verified, it is likely that the strict and specific requirements from credit card companies to encrypt credit card numbers while in storage—and the lack of similar explicit regulatory requirements to encrypt Social Security numbers while in storage—resulted in this inconsistent application of encryption.


Many organizations make it a matter of business practice to do only the minimum required with regard to safeguard implementations, including encryption, unless explicitly, contractually, or legally required to do otherwise. However, organizations should consider the impact of encrypting data in the event an incident does occur. Many current United States state breach notification laws, such as California’s SB1386, do not require organizations to report incidents involving personal information if the data was encrypted. The United States Federal Trade Commission (FTC) has indicated in many of their decisions that a lack of encryption to safeguard data violated regulations or contributed to an unfair and deceptive business practice. For example, in September 2005, the FTC determined Superior Mortgage Company violated the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule because, among other actions, it “did not encrypt or otherwise protect sensitive customer information before sending it by email.”



An excerpt from the FTC’s published Fair Information Practice Principles recognizes the value of encryption as a strong safeguard:

Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

Encryption is one of the most effective security tools available to protect the confidentiality of and access to sensitive data. New encryption solutions have made encryption easier to use and manage as well as more economical than ever before.

 Encryption is specifically stated in several laws—including the Health Insurance Portability and Accountability Act (HIPAA), GLBA, and California SB 1386—as a safeguard organizations must consider.

Encryption Demonstrates Due Diligence

Even Iron Mountain, a company that lost backup tapes containing clear-text information about millions of people for at least four of their customers during the first 4 months of 2005, recommended in an April 22, 2005 report on internetnews.com that organizations should encrypt information on backup tapes. Data should also be encrypted on mobile computing devices as well as on other devices and systems as determined by risk. Encryption is an effective security practice that demonstrates due diligence as well as goodwill for the individuals' personal information.

Organizations need to take a second look at using encryption to protect sensitive data at rest and in motion; particularly if the organization handles confidential information and/or is covered by one or more data protection laws. Remember, when information is unreadable by the unauthorized, breaches from the unauthorized can be avoided.