

Encryption: Not the End-All Fix for Data Privacy

All of the 39 state data-breach laws exempt encrypted data from PR-nightmare public-notice requirements, but don't let that fool you into thinking it's an easy answer to the data privacy challenge. Here's the lowdown on loopholes, caveats and options to consider when applying encryption.

By Philip Alexander
June 1, 2007

Are you prepared for the unthinkable? I'm talking about a security breach involving customer information. Many federal and state data-privacy laws now demand embarrassing and potentially business-damaging public disclosures when a breach occurs, but all such laws make exceptions if that data was encrypted. That might lead you to think that encryption *is* the ultimate privacy safeguard, but you would be wrong.

While encryption is an important step to take for the protection of sensitive data, it's not the end-all fix for data security. Comprehensive data protection requires numerous, overlapping defensive technologies and policies to provide a more complete level of security. Encryption is designed to protect data from unauthorized disclosure, but if the would-be hacker can trick a system to believe that they are an authorized user, encryption can be circumvented.

This article addresses the need to have strong controls around who is granted access to systems that contain sensitive information, such as social security numbers, medical records and the like. It also describes several approaches unauthorized user will try to use to gain access to sensitive information.

The 'Social Engineering' Hack

Social engineering is a low-tech approach where hackers try to trick employees into providing their username and password. Armed with this information, a hacker can access sensitive information, encrypted or not. How willing would your employees be to provide their user account information if they received a call from somebody saying they're from technical support? For publicly traded companies, the names of their most senior executives are freely available on the Internet, and impersonators are all too willing to use them. It's alarming, but most employees would be very willing to answer most questions by people claiming to be calling from the office of a C-level executive.

The Phishing Scam

Hackers will try to trick consumers into giving them sensitive information by sending e-mail messages claiming to be from a company, say a bank or a credit card

company, with whom the consumer has a business relationship. The fraudulent e-mail will advise the consumer to logon to keep their account active, or some other false pretense, but the link will actually take the consumer to the hacker's Web site. Many of the fake Web sites are very professional looking, mimicking a company's actual Web site. Once the consumer enters in their username and password, the hacker has all the information they need to access their account.

Again, all the encryption in the world won't protect a consumer from becoming a victim of a phishing attack. The most effective way to combat both phishing and social engineering is through education and awareness campaigns.

When Encryption is Insecure

Encryption is merely a tool. If used improperly, it can actually cause security problems. Encryption makes data unreadable by running it through a complex mathematical formula and turning into "cipher-text." Encryption can be used to protect data stored on a server or data that is in transit from one system to another. Many companies outsource technical support and other types of services to third parties. To protect sensitive information, transmissions between two parties are often encrypted. This is an important step to protecting sensitive data, but it has to be properly configured. A common approach is to create a secure area just inside the outer edge of a network where you encrypt and decrypt data transmissions before proceeding further. This lets your company see what data the third party is either sending to or taking from your servers.

If a third party is given an encrypted transmission line tied directly to internal systems, that party would be able to bypass perimeter security monitoring devices. With such access, they could perform illegal activities such as embezzlement or just plain hacking. Since the data transmissions are encrypted, they would be able to act in secrecy. Also bear in mind that unlike employee accounts, user accounts for third parties generally aren't associated with a single individual. If ABC company is providing support, their accounts will likely be shared by a number of support personnel. Many service companies also provide "follow-the-sun" support, so they will have locations in different time zones and countries to make it easier to provide 24/7 coverage. Unfortunately, this makes tracking precisely which support person is using what account even more difficult.

Proper Uses of Encryption

There are, of course, many instances in which encryption is a very effective security tool. For mobile employees, hard drive encryption is a great way to protect the data on laptops in the event they are lost or stolen. As the name suggests, the technology encrypts the entire hard drive as opposed to only select folders or files. Thus the end-user does not have to concern themselves with which data should be encrypted. It's all encrypted. One-way encryption, also known as a hash, is often used to

protect passwords. Depending on the specific network topology, password files can be maintained on local systems or on dedicated authentication servers. In either case the password files are often hashed to protect their confidentiality. Since a hash is non-reversible by design, it's considered that much harder to hack. Secure Socket Layer (SSL) is the standard used to provide a level of protection for sensitive data that is transmitted over the Internet.

One challenge businesses face is finding encryption solutions for the wide range of computer systems deployed in their networks. Performance is another encryption challenges as it's CPU intensive and can negatively impact performance.

There are dedicated encryption appliances that are operating-system agnostic. In fact, the need for dedicated, hi-speed crypto-appliances has become so great that the market is flourishing. Many of these vendors tout that they are certified by either the U.S. Government or by major security consortiums such as the National Institute for Standards and Technology (NIST). Vendors in the crypto-appliance market include CipherOptics, Decru and Neoscale, to name just a few.

Dedicated devices are placed right on the network and can encrypt data both in storage and in transit. The CPU-intensive encryption is handled by the appliance, not by your servers, so performance doesn't suffer. Many of these encryption appliances will work with most versions of Windows, UNIX, Linux, mid-range systems such as AS-400's and even mainframes.

Yes, encryption is an important tool to maintain the confidentiality of sensitive data. However, it's not the end-all answer to data privacy. If improperly used, encryption can actually be a security liability, and misuse will eventually impact the exemptions offered in many current data privacy laws.

Philip Alexander is the author of the book [Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers](#) published by Greenwood Publishing