

INFORMATION SECURITY MATTERS

August 2005
Volume 2, Issue 3

Cedric Bennett & Associates ◦ ced@bennettsite.com ◦ 650 858-0883 ◦ <http://bennettsite.com/cba>



Protecting Sensitive Data

These days it seems that not a week goes by in which we don't see at least one article in the news about unauthorized access to sensitive data - particularly personal identity information. Sometimes we hear about computers containing tens of thousands of personal records being compromised through the exploitation of some vulnerability. Other times it may be that secondary storage media, such as backup or archival data tapes, have been mislaid or taken. And still other instances occur when computers, particularly laptops, are stolen.

The efforts aimed at reducing these exploits are both technical and procedural. These approaches are designed to do an effective job at protecting the hardware and media upon which the data is processed and stored. For example, known vulnerabilities in operating systems and applications are corrected or

"An important additional security layer is the protection of the data itself by the application of encryption technologies"

Follow-up on "How Do We Select Security Products?"

In the last issue of *Information Security Matters* (April 2005, Volume 2, Issue 2) I offered an opinion about the selection of information security products at our institutions and then asked for your opinion on the topic. I'm pleased to say that many of you took the time to respond - thank you very much. As prom-

Inside This Issue

Protecting Sensitive Data	1
Follow-up on "How Do We Select Security Products?"	1

patched, protective software and hardware devices are used to make it much harder for criminals to access the devices upon which the data is stored, and procedures are implemented aimed at reducing the exposure of data stored on portable devices.

Of course, it is important to pursue all these efforts - generally speaking, anything we can reasonably do to reduce sensitive data exposure and prevent it from falling into the wrong hands should be done. It is axiomatic in information security circles that nothing can be made 100% secure. That is why information security experts will encourage the practice of defense-in-depth - applying layers of security in an effort to make it much more difficult for crackers (*criminal hackers*) to access or damage important information assets.

An important additional security layer is the **protection of the data itself** by the application of encryption technologies. Encryption is a process which converts information into a

Please see *Protecting* on page 2

ised, here is a summary of that input.

First of all, many of you were in agreement that at your institution, the information security product that would most likely prevail in a competitive selection would be the one that met the particular pain-point at the most rea-

Please see *Select* on page 2

Protecting from page 1

form that is unreadable by unauthorized individuals. Once data is encrypted it cannot be converted back into a clear (i.e., understandable) form without access to the specific key that will allow it to be decrypted. Therefore, even if criminals obtain sensitive data through the exploitation of vulnerabilities, because of storage media mishandling, or even by access to a stolen device, the data so obtained is useless to them since it cannot be correctly interpreted without the decryption key.

Data encryption is already in use today in many systems, particularly those which process online transactions. For example, most web sites that accept orders for merchandise and services use techniques that automatically cause any transmitted information to be encrypted as it leaves the source computer and then to be decrypted when it arrives at the target system. Many business and administrative systems use similar automated encryption/decryption approaches to protect entire files of data while they are in transit across the Internet.

What are used less frequently, unfortunately, are techniques that encrypt data that is stored. As a result, even though sensitive data is protected by encryption while it is in transit, that same data can be more vulnerable to unauthorized access approaches once it is "at rest" on some computer or archival media.

Protecting stored data via encryption is not overly difficult; however, establishing workable processes that allow for safe decryption of that data can be more complex. Generally speaking, one would only want to allow for automated decryption (and re-encryption of authorized changes) to stored data when it is

certain that other very strong protection mechanisms are in place to prevent unauthorized access. Such techniques are beginning to be used more and more to protect large, central stores of data at our institutions and businesses.

What is not yet happening nearly enough is the application of similar technology to local computers, particularly laptops. An important additional step that should be taken by our institutions is encouraging, supporting, and even providing for the use of encryption software for desktop and especially laptop computers. If more of our laptop computer users were using encryption to protect sensitive data, we'd be seeing fewer newspaper headlines about lost or compromised data. ♥

Select from page 1

sonable price, without much regard for additional, but otherwise non-requested features.

On the other hand, several of you felt that your institution's were more enlightened than that and were willing and able to be convinced that the product with the longer term strategic value, that also accomplished the immediate goal, should be selected. Some indicated that this was even more likely if the person responsible for information security was motivated sufficiently to provide the leadership to make this happen.

One reply offered an additional interesting twist on this latter notion - to wit, if the person responsible came to the information security position with knowledge of a particularly effective tool, it would be even more likely that such an individual would be able to convince others at that institution to proceed with the implementation of that product. ♥