

Looking for Privacy in All the Wrong Places by George Tillmann

12/21/06

a strategy+business exclusive

Looking for Privacy in All the Wrong Places

Executives must protect valuable corporate and personnel data to avoid a potentially crippling attack.

by **George Tillmann**

Data theft is a potentially disastrous threat to organizations of every sort, yet executives have long been content to let it be someone else's problem. That could soon change.

With the incidence of such crimes on the rise, along with consumer outrage — more than 180 million computer files containing such sensitive information as Social Security numbers, birthdates, credit card numbers, and financial or medical histories have been poached since early 2005 — legislators around the world have introduced bills that would hold organizations more accountable for safeguarding confidential information. In the United States, the most punitive proposed law, sponsored by Senators Arlen Specter, Republican from Pennsylvania, and Patrick Leahy, Democrat from Vermont, would require that companies with at least 10,000 digital files on individuals design a security system to protect sensitive records from unauthorized access. In addition, these companies would have to publish their data privacy procedures and conduct routine audits to evaluate vulnerabilities. Failure to follow these rules would result in fines and possible federal prosecution.

If this bill passes in anything near its current form, it could have a Sarbanes-Oxley-like effect on companies. Faced with this possibility, CEOs can no longer neglect the potential impact of data theft on customer loyalty, Wall Street confidence, shareholder support, litigation, and regulatory compliance.

The information technology departments of many corporations have been trying to get ahead of data theft for more than a decade. Encryption — the scrambling

of data using a secret key — continues to be the standard approach for protecting information that travels over the Internet or is sent outside the company's protective firewall to remote laptops, PDAs, and cell phones. Intercepting transmitted data is still perceived as the primary threat. In most companies, it remains the area of greatest security focus. But it is also the least likely way data will be lost or stolen.

Data can be viewed as existing in one of two states: dynamic (or moving) and static (or fixed). For every transaction involving dynamic data, there are millions of records in a static mode sitting on hard drives, magnetic tapes, CDs, and DVDs, in memory sticks and cards, and in mobile equipment like laptops, PDAs, and BlackBerrys. These records are almost never encrypted. So it is not really surprising that most data theft isn't the work of hackers breaking into corporate networks. Digital thieves most often intercept unencrypted static data as the hardware it is stored on travels to remote storage sites, or they steal the data from portable devices.

In the last 18 months, dozens of organizations have been victimized in this way. In May, it was revealed that the U.S. Department of Veterans Affairs lost 26.5 million military records stored on a laptop that was stolen from the home of an agency employee. This came on the heels of similarly low-tech incidents at Wells Fargo, Ernst & Young, Fidelity Investments, the University of Pittsburgh Medical Center, and the University of Washington Medical Center.

Nevertheless, IT units have, on the whole, chosen to leave static data unencoded. Meanwhile, the urgent need to address this vulnerability continues to grow.

George Tillmann

(tillmann_george@bah.com) recently retired from Booz Allen Hamilton, where he was a vice president. He spent his first 17 years at the firm as a management consultant specializing in information technology and his last five years as its chief information officer. He now helps CIOs manage their IT organizations.

While so many files remain unencrypted, the cost of computer storage is plummeting, allowing organizations to maintain vast amounts of data for longer periods of time more cheaply than ever before. Many companies now house multiple terabytes of data (one terabyte is 1,000 gigabytes), and petabyte volume is just around the corner. That's a lot of data sitting defenseless.

The main reason is that it's more expensive to protect static data than dynamic data because it involves modifying the hardware or software on every storage device. To encrypt data on personal devices, such as personal computers, the encryption software is usually inserted between application programs and the disk drives. As data is recorded on the storage device, it is intercepted and encrypted, and the encoded information is written to the disk. The cost of adding encryption to individual PCs and mobile equipment could exceed the cost of encrypting the company's entire data center. And businesses traditionally balk at paying for infrastructure initiatives when they see little functional benefit.

Moreover, encryption of stored data carries significant risks. If the decryption of a transaction involving dynamic data fails, resulting in a mishmash of the original message, the data can be resent. But when the decryption of a disk drive goes wrong — an infrequent but nonetheless disturbing prospect — in most cases nothing can be done unless there is an unencrypted backup stored elsewhere. Few IT executives would relish telling a user that the 40 gigabytes of data on his or her laptop are unrecoverable. Moreover, encryption can slow performance of PCs by anywhere from 1 to 20 percent, depending on implementation, so user dissatisfaction can become a significant issue.

But those problems are minor compared to the threat of data theft. With breaches occurring literally every week, few senior managers can afford to do nothing. The situation is analogous to that of the late 1990s, when the Y2K threat presented an IT problem urgent enough to require senior management involvement to marshal the resources necessary to complete the task.

If protecting static data isn't already a high priority for corporate leaders, it needs to become one — and fast. Theft of data can be catastrophic: It can destroy the trust a company has built with its customers, negatively affect earnings, and result in intervention by regulators or prosecutors, which could be costly. With so much at stake, the responsibility for leading the effort to safeguard confidential information must reside at the highest levels of the organization.

To minimize data theft, CEOs should oversee an enterprise-wide initiative that includes:

- Implementing stringent corporate information retention policies and processes. These rules should state explicitly what data can be stored, where it can be stored (on PCs, laptops, PDAs, etc.), and how (encrypted or not) it should be stored. The policies need to address all types of data (customer, employee, and supplier records), not just financial information, and they should include guidelines for getting rid of obsolete information as soon as it is not needed, to reduce the amount of information stored.
- Allocating resources, such as money, staff, and time. This will likely require postponing other IT work. CEOs must be vigilant that the data security program should at no point be put on the back burner while more popular projects are completed.
- Running interference. Users need to be told explicitly that the decision to protect sensitive data comes from the CEO and that IT management is simply the CEO's agent for implementation.

The best guess is that in five to seven years, all data — be it stored in a data center, on tapes sent by messenger to off-site storage, on laptops, cell phones, PDAs, or who knows where — will be encrypted. But before then, many organizations will suffer embarrassing data losses and information theft. Smart CEOs will act now before they are victimized; others will pay the price for dismissing the vital importance of keeping data private. +

strategy+business magazine
is published by Booz Allen Hamilton.
To subscribe, visit www.strategy-business.com
or call 1-877-829-9108.