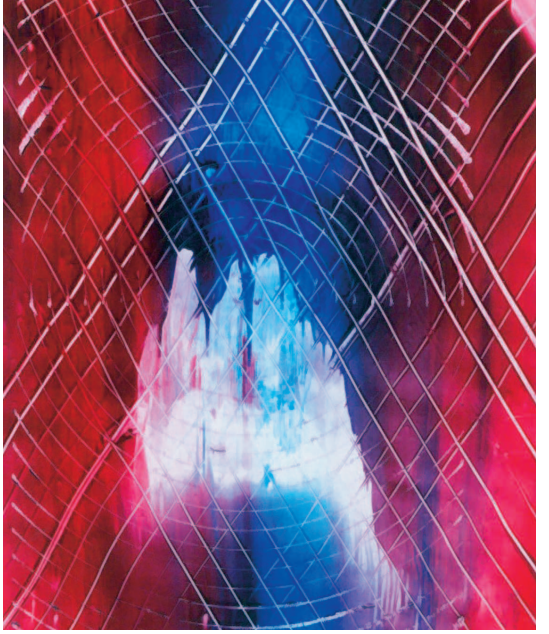
The Impact of Personally Identifiable Information

Linda Wilbanks



In May 2006, someone stole a US Veterans Affairs Department laptop containing 26.5 million personal records. It was an unprecedented loss of personal information. Nine months later the VA lost a hard drive containing sensitive information on physicians who had submitted bills to Medicare and Medicaid. Shortly thereafter another hard drive was lost from an Alabama facility containing medical data on 535,000 VA patients.

Many other agencies have suffered through the consequences of lost hardware containing sensitive information. But losing hardware is not the only way to lose sensitive personal information. In April 2007, hackers attacked Missouri University's computer network and released the social security numbers of more than 22,300 current and former Missouri students. This was the second breach of the university's computer system in the past year. The US Department of Agriculture recently acknowledged that for years, its Web site inadvertently exposed the personal information of 38,700 people. Personal information can include your financial data, your medical data, and, basically, your virtual identity. All valuable data could easily lead to identity theft and no one seems safe.

We all have an obligation to protect personal information, but what does that mean to you as an individual or as an IT manager?

US LEGISLATION STEPS IN

In May 2007, US Representative Tom Davis, a ranking member of the House Oversight Committee, introduced the Data Breach Protection Bill that will require the government to better protect the personally identifiable information (PII) it collects from citizens and inform them if this information is lost or stolen. The US Congress plans to continue work on the requirements for the private sector. The Privacy Act and E-Government Act of 2002 outlined the parameters for protecting personal information, but the Data Breach Protection Bill would require the executive branch to establish practices, procedures, and standards for agencies to follow if the PII is lost or stolen and if there is a reasonable risk of harm to an individual. This bill will have a unique impact on chief information officers—it will give them the authority, when appropriate, to ensure agency personnel comply with all information security laws.

Separately, the Senate Judiciary Committee has approved two data security bills—the comprehensive Personal Data Privacy and Security Act of 2007—and the more narrowly tailored Notification of Risk to Personal Data Act, introduced by US Senator Dianne Feinstein.

The Clinger Cohen Act of 1998 established the requirement that federal agencies must have a CIO. It established the general responsibilities for the CIO as providing advice to the head of the agency to ensure information technology is acquired and managed within an architecture and meets established requirements. The act defines information technology to include computers, ancillary equipment, software, firmware, support services, and related resources. It also identifies the storage, interchange, and reception of data or information as part of IT.

The role of the CIO has evolved to a strategic leader, participating in the development of the visions for the company instead of just implementing the nuts and bolts of technology. But the question in the back of many people's minds, including legislators and CIOs, is do they have the authority to act? This new bill, if passed, will make this clear, giving CIOs that authority.

But what exactly is the PII that this bill refers to? On 12 July 2006, Karen Evans, the administrator for the Office of E-Government and Information Technology within the Office of

Management and Budget (OMB) issued a Memorandum for Chief Information Officers. The memo coined the phrase *personally identifiable information* and identified an agency's responsibility for reporting incidents involving PII. In the memo, PII is defined as

> any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace individuals' identities such as their name, social security number, date and place of birth, mother's maiden name, biometric records, and so on; it includes any other personal information which is linked or linkable to an individual.

The memo also stated a new procedure requiring all agencies to report all incidents involving PII to the US Computer Emergency Readiness Team (see http://www.us-cert.gov) within one hour of discovering the incident. However, the memo did not clarify whether an "incident" is a suspected breach or a confirmed breach.

In a memorandum to the heads of departments and agencies, issued on 23 June 2006, Clay Johnson III, Deputy Director for Management within OMB, noted that the protection of sensitive agency information is outlined through a series of recommendations from the OMB. These include encrypting all data on mobile computing devices, allowing remote access only with two factor authentication, and using a time-out function for remote access.

So, how do CIOs enforce PII? First, don't fall into the misconception that if you are not part of the government, you don't have a responsibility when it comes to protecting the personal information of people. Congress is working on legislation that will address the public sector, but people also expect their PII to be protected. Identify theft is real. The Federal Trade Commission reports that identity theft topped the list of consumer complaints, accounting for 42 percent of all complaints lodged in 2004, up from 40 percent in 2002. The FTC also reported that approximately 10 million American consumers discovered that unauthorized individuals used their personal information to open fraudulent bank, credit card, or utility accounts, or to commit other crimes. People expect that if you have their information that you will protect it.

CIO'S MISSION: PROTECTING INFORMATION

As a group, what should we do to protect PII? The first obvious solution is to ensure that any computer—portable or desktop—containing PII has the appropriate hardware and software safegaurds installed. Data on any computer, portable device, handheld, and thumb-drive type device must be encrypted during transmission or while at rest. In the event that the device is lost or hacked, the data should not be easily readable.

IT Professional (ISSN 1520-9202) is published bimonthly by the IEEE Computer Society. IEEE Headquarters, Three Park Avenue, 17th Floor, New York, NY 10016-5997; IEEE Computer Society Publications Office, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; voice +714 821 8380; fax +714 821 4010; IEEE Computer Society Headquarters, 1730 Massachusetts Ave. NW, Washington, DC 20036-1903. Annual subscription: $40 in addition to any IEEE Computer Society dues. Nonmember rates are available on request. Back issues: $25 for members, $102 for nonmembers. Postmaster: Send undelivered copies and address changes to IT Professional, Circulation Department, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855. Periodicals Postage Paid at New York, N.Y., and at additional mailing offices. Canadian GST #125634188. Canada Post Corp. (Canadian distribution) Publications Mail Agreement #40013885. Return undeliverable Canadian addresses to 4960-2 Walker Road; Windsor, ON N9A 6J3. Printed in USA.

Editorial: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in *IT Professional* does not necessarily constitute endorsement by the IEEE or the Computer Society. All submissions are subject to editing for style, clarity, and space.

Because we're responsible for protecting this data, we need to look further. Questions to ask include why is that PII on that device? And, does it have to be there for the owner to do his or her job? Often PII is on a machine while users work on a file. When they complete the task, users send the file across a network but the information continues to reside on the machine, providing the potential for it to be stolen through hacking or loss of equipment.

Another more comprehensive, but not as obvious, solution is to determine whether users really need a portable device as part of their job. Does their job require them to work after hours, or do they travel extensively and need the laptop to do their work? Many hotels now offer computers for guest use, often free of charge. Is data on an encrypted thumb drive sufficient, or is a laptop needed?

Finally, in the event your company does experience a loss of data, the name of the game according to Eric Denzenhall, a crisis management expert, is damage control, not damage disappearance. You cannot reverse the loss; you need to lessen the impact, quantify the problem, and quickly determine the extent of the damage. These principles apply regardless if you are dealing with the loss of financial information or health information. People need to be reassured that the situation is under control and that it won't happen again. They really don't care how it happened or which system was lost or breached—they just want to be reassured that their information is safe. A strong, honest leadership is key to overcoming data loss.

As CIO and IT managers, we need to start looking outside the box to prevent the loss of PII. This means looking beyond hardware and software solutions to the personnel solutions that might result in an improved quality of life, with less work outside the office. For example, do we need to take home the laptop containing a personnel file and work on it after hours, impacting our down time and family time? Do we need to work on emails after hours discussing work, including PII in our emails, or can they wait until we get back to the office? Let's stop and look at what we are emailing and the work we are taking home. ■

Linda Wilbanks *is CIO of the US National Nuclear Security Administration. Contact her at Linda.Wilbanks@nnsa.doe.gov.*

If you would like to write an article for CIO Corner, please contact IT Professional *at itpro@computer.org.*

For further information on this or any other computing topic, please visit our Digital Library at http://www.computer.org/publications/dlib.