Sorting diamonds from toothbrushes: New guide to protecting personal information

January 13 2009

Thefts of personally identifiable information (PII), such as social security and credit card account numbers, are increasing dramatically. Adding to the difficulty of fighting this problem, organizations often disagree on what PII is, and how to protect it. Now, in a first-of-its-kind publication, the National Institute of Standards and Technology has issued a draft guide on protecting PII from unauthorized use and disclosure.

“You can’t protect PII unless you can identify it,” says NIST’s Erika McCallister, a co-author of the new work. The new NIST publication provides practical guidelines for implementing a basic definition of PII established by the government’s Office and Management and Budget (OMB) in a 2007 memo: “information which can be used to distinguish or trace an individual’s identity”* either all by itself—such as fingerprints, which are unique—or in combination with other information, such as date of birth, which can belong to multiple people but can be narrowed down to an individual in connection with other data.

Echoing former national security advisor McGeorge Bundy, who once stated, “If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds,” McCallister and her co-authors observe that, “All PII is not created equal.” A telephone area code holds less specific information about an individual than a social security number, so “you don’t need to protect things the same way,” McCallister says.

The NIST team recommends tailoring safeguards to the level of risk involved in holding personal information. PII should be graded by "PII confidentiality impact level," the degree of potential harm that could result from the PII if it is inappropriately revealed. For example, an organization might require appropriate training for all individuals who are granted access to PII, with special emphasis on moderate- and high-impact PII, and might restrict access to high-impact PII from mobile devices, such as laptops and cellphones, which are generally at greater risk of compromise than non-portable devices, such as desktop computers at the organization's headquarters.

The publication also recommends basic actions that organizations should take: identify all the PII they maintain, minimize the amount of PII they collect to what is strictly necessary to accomplish their mission, and develop incident response plans to handle breaches of PII. Such plans would include elements such as determining when and how individuals should be notified, and whether to provide remedial services, such as credit monitoring, to affected individuals.

The publication is intended primarily for U.S. federal government agencies, which must implement certain requirements on handling and protecting PII, but is intended to be useful to other organizations. The publication, known as Special Publication (SP) 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," is available at the NIST Computer Security Resource Center's draft publication Web page: csrc.nist.gov/publications/PubsDrafts.html#800-122 .

Source: National Institute of Standards and Technology

Citation: Sorting diamonds from toothbrushes: New guide to protecting personal information