Principles for Protecting Your Organization's Information Assets

According to the Identity Theft Resource Center, nearly 58 million records were reported compromised in the United States last year – 40 million of them from Target customers during the Christmas shopping season.

At $188 per record, according to Ponemon Institute's "2013 Cost of Data Breach Study: Global Analysis," the direct cost of a data breach can have a huge impact on the bottom line. Other costs due to customers' loss of confidence could supply a knockout punch. Target reported that its 2013 fiscal fourth quarter profits were down $440 million due to its breach.

As a professional with responsibilities around safeguarding your organization's information assets, you'll find plenty of help in this issue of *Information Management (IM)* and the *Hot Topic* that is tipped inside.

In our cover article, Virginia Jones, CRM, FAI, provides an overview of U.S. federal privacy laws and their information governance implications. A comprehensive discussion of these laws is available in her ARMA International Educational Foundation report "Requirements for Personal Information Protection, Part 1: U.S. Federal Law," available at *www.arma.org/bookstore.*

Any organization that has international customers must also be concerned about other countries' legislation. Experian's "2014 Data Breach Industry Forecast" predicts that the rise of the cloud, which allows data to move seamlessly across borders, and the EU regulations that "will be enforced based on where the customer lives, rather than where the data is located," will lead to an increasing number of complex information-related violations. Google recently found out how expensive this can be, as France levied the maximum fine possible under French law – €150,000 ($205,000 U.S.) – against it for violating its privacy law.

Cherri-Ann Beckles covers this terrain in her feature article, "Managing Privacy in Recordkeeping Systems: An International Perspective." Among other advice Beckles gives, she writes, "Classification schemes that group record series containing personal data in logical, functional categories, could be used as the foundation on which sound data protection strategies are built."

For those developing or revising classification schemes, the case study written by Kathryn Scanlan, J.D., CRM, "Procedures for Developing an Electronic File Plan," will be a valuable resource. In addition to discussing the use of folders to control access, as Beckles suggests, the case study covers how to initiate the project, whom to involve, and how to design and implement the structure. It also provides a variety of sample file structures.

Auditing the RIM program is a critical aspect of ensuring that information is properly protected.

INFORMATION MANAGEMENT
AN ARMA INTERNATIONAL PUBLICATION
MARCH/APRIL 2014
Protecting Information Privacy
Per U.S. Federal Law
Page 18
Procedures for Developing an Electronic File Plan
Page 28
An International Perspective on Protecting Personal Information
Page 34
STOP
Special in this issue:
hottopic
SECURING INFORMATION
Strategies for Cradle-to-Grave Protection

Our RIM Fundamental series article, which was excerpted from ARMA International's just-published *Auditing for Records and Information Management Program Compliance* (ARMA International TR 25-2014), identifies "The Elements to Be Assessed in a RIM Audit."

Of course, basing a RIM program on the Generally Accepted Recordkeeping Principles® (Principles) is the most comprehensive way to ensure information protection. Julie Gable, CRM, CDIA, FAI, developed two case studies that show the Principles in practice for new RIM programs.

We aim to provide practical help in every issue of *IM*. Please e-mail *editor@armaintl.org* to tell us what topics would be of the most value to you!

Vicki Wiler
Editor in Chief