HABIF, AROGETI & WYNNE, LLP
Certified Public Accountants and Business Advisors

Protecting Personal Information through GAPP Implementation

By Dan Schroeder, Partner

With identity theft on the rise-there were 8 million incidents reported in 2010--the business risks associated with internet--based applications and the management of clients' or customers' personal information are increasing significantly. The generic term "personal information" is used here to represent personally identifiable information (PII), sensitive information, and other information that is or could be subject to regulatory or statutory compliance requirements.

State, Federal, and international governments are expanding compliance regulations concerning personal information. In the U.S., Congress is considering no less than five bills that would establish nationwide standards for the security and privacy of consumers' personal information and 46 states have already enacted some form of privacy regulation. The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) have adopted a Generally Accepted Privacy Principles (GAPP) framework that brings together current national and international privacy regulatory requirements and best practices. The overall objective of GAPP is to ensure that the collection, use, retention, disclosure, and disposal of personal information conform with the commitments in an entity's privacy notice and with specific criteria set forth in GAPP.

There are five primary steps a business should consider when preparing to deploy GAPP. We've also included an optional sixth step for service organizations.

Step 1: Conduct a Data Inventory. A business should consider compiling and maintaining an inventory of personal data collected and/or processed, segmented by privacy nexus requirement (jurisdictional; i.e., state, country level, and/or regulatory; e.g., GLBA, HIPAA). Understanding the data associated with personal information is useful for identifying the processes that involve or could involve personal data, and the owner of those processes. Businesses may find it helpful to prepare a flowchart that depicts the flow of personal information, including inputs, processing, points of storage, outputs, personnel and/or third parties' that are involved in various aspects of the flow, as well as who could access the personal information. This documentation of the data flows can also be a very useful means of identifying any points in the data flow that represent significant inherent risks and whether mitigating controls exist for those risks.

Step 2: Complete a Risk Assessment: Identify inherent operational risks associated with the protection of personal information, and whether appropriate mitigating controls exist.

Step 3: Assess compliance against GAPP criteria: Review the company's existing privacy management policies, procedures, and control functions relative to the specific criteria defined by the AICPA GAPP framework.

Step 4: Establish GAPP-based controls: This step involves management addressing any control gaps identified in the GAPP Compliance assessment step. The organization should update the GAPP Assessment report and policies and procedures as appropriate to reflect controls accurately as they are updated or changed.

Step 5: Monitor GAPP controls: Management should monitor a wide range of compliance considerations, as well as complaints or potential instances of non-compliance, and prepare required or recommended reports.

Optional Step: Obtain Independent Attestation: Service organizations that provide personal information-related services on behalf of other user entities often need to provide those user entities with an independent auditor's assurance report related to the organization's privacy risk management practices. Under AICPA Statements on Standards for Attestation Engagements, the independent auditor may report on either management's assertion or the subject matter of the engagement.

Protecting the personal information of your clients and customers is a business imperative. Habif, Arogeti & Wynne is ready to help you develop or improve your information controls to meet your business goals and to meet your customers' expectations of privacy and protection. For more information, visit our Privacy Risk Management Services page on our web site or contact Dan Schroeder.

Dan is a partner at Habif, Arogeti, & Wynne, LLP (HA&W) in Atlanta, GA and is the current chair of the AICPA's IT Executive Committee. He is responsible for HA&W's IT audit and risk advisory services including Service Organization Control Reporting, privacy risk management, data management, and IT Governance.