

PREVENTING DATA BREACHES

By Nicholas F. Cheung

Companies that implement a privacy breach management program are ahead of the curve when it comes to protecting data

Ensuring that organizations have a privacy incident and breach management program in place is a key enhancement to *Generally Accepted Privacy Principles* (GAPP). GAPP is an internationally recognized privacy framework developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

“Having a privacy breach management program in place is critical in ensuring that appropriate actions are taken following a breach,” says Everett C. Johnson, CPA, chair of the AICPA/CICA Privacy Task Force and a past international president of ISACA. “These actions would include assessing the severity of the breach, identifying what actions are necessary to stop the breach and determining whether individuals and/or regulatory authorities need to be notified.”

With breach notification in provinces, such as Alberta, soon to become a reality and a breach notification amendment to the federal *Personal Information Protection and Electronic Documents Act* expected soon, organizations should take the time now to ensure they have done everything they can to prevent such breaches — such as reviewing their compliance with GAPP — and if one does occur, ensure that their breach management program is in place and ready to go. In addition to the significant monetary costs in responding to a breach, an organization can also suffer from:

- Damage to reputation, brand or business relationships;
- Liability resulting from identity theft;



- Lost business and reduction in market share; and
- Increased monitoring from privacy commissioners.

GAPP, last updated in 2006, are designed to help an organization’s management develop a program that addresses their privacy obligations and risks and to assist them with assessing their existing privacy program. It is also the basis for a privacy audit that can be performed by a Chartered Accountant (CA). GAPP contains 10 principles that are each supported by objective, measurable criteria for handling personal information throughout an organization. Together, this set of privacy principles and related criteria are useful to chief privacy officers, executive management, compliance officers, legal counsel and CAs offering technology advisory services and privacy consultants.

The changes, which include eight new criteria (now 73 in total) and the modification of two others, were the result of deliberations and consideration given to comments received from the public in response to the exposure draft that was released in March 2009. “Safeguarding personal information is one of the most challenging responsibilities an organization has, whether it’s information pertaining to employees or customers,” explains Johnson. “We’ve updated the criteria of our privacy principles to minimize the risks to personal information.”

The new criteria include:

- Identification and classification of personal information;

- Privacy risk assessments;
- Privacy awareness and training;
- Information developed about individuals;
- Disposal, destruction and redaction of personal information; and
- Personal information on portable media

“Ensuring that employees are educated about privacy will help prevent privacy breaches, improve customer service and demonstrate the organization’s commitment to sound business practices,” explains Donald Sheehy, CA-CISA, CIPP/C, associate partner with Deloitte (Canada) and a Canadian member of the AICPA/CICA Privacy Task Force.

The frequency with which portable devices that contain personal information, such as laptops and USB memory keys, are being lost highlights the need for organizations to be proactive and vigilant in this area. In December, an unencrypted USB key containing the health information of more than 84,000 patients who attended H1N1 vaccination clinics in Ontario’s Durham Region was lost.

“Portable devices, such as laptops and memory sticks, provide convenience to employees but appropriate measures must be put in place to properly secure them and the data they contain,” relates Sheehy. “We must stay abreast of technological advances to ensure that proper measures are put into place to defend against any new threats.”

Several organizations worked in conjunction with the AICPA and CICA on GAPP, including ISACA and the Institute of Internal Auditors. It is available in two versions, one for business management and one for CAs in public practice, who provide consulting and attestation/audit services. ■

Nicholas F. Cheung, CA, CIPP/C (nicholas.cheung@cica.ca) is a principal with the Canadian Institute of Chartered Accountants and a member of the AICPA/CICA Privacy Task Force. Generally Accepted Privacy Principles are available, free of charge, from www.cica.ca/privacy.