

Canada develops guide to help stop data leaks

String of high-profile breaches prompt move

By Gloria Gonzalez, Business Insurance

OTTAWA - Canadian companies now have a risk management tool to help them respond to breaches of personal information: new guidelines issued by Canada's federal privacy commissioner.

While the guidelines are voluntary, Canadian organizations can use them to minimize reputational or legal risks related to data breaches and prevent passage of legislation that would make customer notification mandatory, experts say.

The guidelines resulted from a five-year review of Canada's Personal Information Protection and Electronic Documents Act, which sets standards for the collection, use and disclosure of personal information in the course of commercial activities (*BI*, Sept. 18, 2006). High-profile breaches of personal information spurred legislators and regulators to examine developing guidelines or a law outlining the management of data breaches.

Privacy Commissioner of Canada Jennifer Stoddart earlier this month released the guidelines that outline key steps in responding to a breach: containing the breach, evaluating the risk associated with it, notifying affected individuals and preventing future breaches (see story, page 18).

"They're best business practices," said Steven Lingard, assistant general counsel for the Toronto-based Insurance Bureau of Canada, which represents property/casualty insurers and consulted on the privacy guidelines. "If you're a risk manager at a company and you were asked to develop guidelines, you would probably come up with these four steps."

Privacy experts say Canadian organizations must prepare for data breaches, which generated 424 complaints to the federal privacy commissioner's office in 2006, up from 400 in 2005, according to its annual report.

"Really these guidelines do represent a risk management approach and good organizations will make them a part of their business continuity plans," said Drew McArthur, vp, corporate affairs and compliance officer for Vancouver, British Columbia-based TELUS Communications Inc. and a key participant in developing the guidelines.

The guidelines can help mitigate a critical risk for companies experiencing data breaches—potential harm to an organization's reputation or brand by mismanaging the situation. "That's really where the big potential problems occur because once customers decide you can't be trusted, it's difficult to get their trust back," said Mark Hayes, a Toronto-based partner with Blake, Cassels & Graydon L.L.P. who consults on privacy issues.

Class action lawsuits against companies experiencing data breaches is another exposure. "Certainly, there's the possibility of liability issues and that is something organizations are taking quite seriously, although so far in Canada there have been no situations where organizations have been found liable for data breaches," Mr. Hayes said.

The most controversial aspect of the guidelines is the absence of mandatory notification of consumers in all instances of a data breach, observers say. Data breaches should be considered on a case-by-case basis with the key consideration being whether notification is necessary to avoid or

mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed, according to the guidelines. For example, if a company laptop containing encrypted information were to be lost or stolen and subsequently recovered but the information had not been tampered with, notification may not be necessary, the guidelines say.

Several consumer groups withdrew support in favor of a legislative response because the guidelines do not mandate consumer notification in all data breaches. The Public Interest Advocacy Centre, for example, expressed concern that notification was left to a company's discretion, arguing that companies are not in a good position to judge potential harm to their customers and that their commercial interests could factor into notification decisions, said John Lawford, counsel for the Ottawa-based consumer group.

Notification, though, is not always in individuals' best interests, according to companies and business associations involved in the consultation process. Consumers could be desensitized to potential risks if they receive a flurry of data breach notifications and might ignore situations that would require them to take action, privacy experts say. On the flip side, individuals notified of a data breach may take unnecessary action, such as canceling credit cards, they say. In addition, mandatory notification could give potential criminals insight into the value of the stolen information.

"If you had to notify in those circumstances, what you're doing is creating more harm to the individual," said Frank Zinatelli, a Toronto-based vp and associate general counsel for the Canadian Life and Health Insurance Assn., which participated in the consultation process.

PIAC rejected these arguments, saying consumers have the desire and right to know if any of their personal information is breached. "It's better for them to know so that they can take precautions" such as monitoring their credit reports, Mr. Lawford said.

Many organizations, including TELUS, voluntarily notify customers of data breaches even in circumstances that do not meet the threshold in the guidelines. Mr. McArthur said. "We have undertaken notification in very benign circumstances and it's more to cement the relationship with the customer."

Canadian companies are expected to comply with the voluntary recommendations, particularly in light of the number of data breaches in Canada, the risks they present and the "common-sense" approach of the guidelines, privacy experts say.

Widespread compliance could stem the movement toward mandated breach notification, which Ms. Stoddart, several legislators and consumer groups that include PIAC are still promoting, privacy experts say.

"The Canadian experience has been so far that guidelines work well in this country," said Ariane Siegel, a partner in the technology industry group of Gowling Lafleur Henderson L.L.P. and a member of the Information Technology Assn. of Canada, which consulted on the guidelines. "We don't always need statutes and regulations to tell us what to do."