Session title: Best Practices for Protecting Your Agency's Information & Responding to Privacy Breaches
Moderator / Panelists :
Jonathan Batty, Director of Compliance and General Counsel, Elections Ontario
Beth DeWitt, Manager, Enterprise Services and Chief of Staff, Technology Risk Solutions, Deloitte,
Boris Perron, Analyste-Enquêteur, Commission d'accès à l'information du Québec
Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada
Peter Gzowski, Assistant Chief Electoral Officer, Nova Scotia
Date and time : Tuesday December 10 2013, 13 : 45 pm
Rapporteur : Rosalie Readman

Session Summary

The session began with a general discussion of the media attention that privacy breaches attract and whether or not the adoption of new technologies place organizations at greater risk.

Organizations must place a high priority on protecting information if they want to be prepared to manage eventual critical situations that involve the loss of information. The panelists noted that preparation and anticipation are the keys to success when it comes to protecting sensitive data. Organizations must prepare carefully for this type of eventuality. It is of course important to put in place processes that minimize the risk of loss of information, but that in itself is not sufficient. Organizations must also establish processes to manage information loss in order to control the situation, limit damage, and maintain public trust.

In terms of developments in the field of protecting sensitive data, panelists emphasized that there is a movement toward mandatory disclosure in cases of loss. This process is currently voluntary at the federal level in Canada. Panelists also noted citizens' significant concern with protecting their private lives, despite their wavering level of trust in institutions and the ability of these institutions to achieve this objective.

The discussion noted that privacy breaches often occur when temporary projects, outside of standard businesses, are undertaken by organizations.

One panelist presented a very comprehensive four-step action plan designed to manage the loss of confidential information. First, one has to be able to control the risk of further information loss, determine who will take charge of the investigation, and decide who must be apprised of the internal leak. Second, one must assess the size and nature of the violation and anticipate the impact on those persons affected by the loss. This may, for example, require expert forensic investigation advice. Third, one needs to determine how and when the

people affected by the leak will be notified. For example, will they be notified through the media or as part of a more individualized notification process? How quickly should they be notified? What should people be told to do? Are there other people on the outside who must be informed, such as a privacy commissioner or police authorities? Fourth, one must re-examine the systems and processes that were initially put in place to protect information in order to take remedial action and prevent further leaks.

The panelists also noted that it was useful to contact and obtain advice from the agencies and commissions responsible for privacy protection in their respective jurisdictions with respect to procedures and best practices.

Panelists also highlighted the importance of practice as regards the processes put in place to manage information loss. In this regard, carrying out a simulation will truly put to the test the preparations made to implement such a process and help identify the resource persons with whom to collaborate, both within the organization affected and within bodies tasked with regulating protection of information. Most importantly, the discussion noted that the best protection to mitigate against privacy breaches is to incorporate “privacy by design” principles in the design of processes handling information. This is an important business efficiency as responding to a privacy breach can often be costly in terms of the time and resources such issues consume. Finally, apart from these material concerns, there was discussion about how such occurrences can have a serious toll on the morale of an agency and can endanger the public’s confidence in the work of the agency.

There was also discussion about where citizens could be referred to provide credit and identity theft monitoring services. Such services include:

TransUnion – www.transunion.ca
Equifax – www.consumer.equifax.ca
All Clear – www. Allclearid.com (USA)
Experian – www.experian.com (USA)