Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

News Release

For Immediate Release
Jan. 28, 2015

Improvements recommended in report on government privacy breaches

VICTORIA—The B.C. government should build on the fundamentals it has established and make improvements in the way it manages privacy breaches of citizens' personal information, according to a report by B.C. Information and Privacy Commissioner Elizabeth Denham.

"Today is international Data Privacy Day, and privacy breaches are a growing concern for the public. On a daily basis we hear about new ways in which hackers have accessed our private information, about work laptops being stolen out of cars, or cases where human error has put individuals at risk for identity theft and other reputational harms," said Commissioner Denham.

"Government is trusted with a large amount of sensitive personal information, and citizens expect that appropriate safeguards are in place to protect it. With this in mind, I decided to conduct a review of the efficacy of the government's breach management practices, which is an essential part of any privacy management program."

A privacy breach occurs when someone without proper authority obtains access to personal information, through the loss, theft, or other means of inappropriate collection, use, or disclosure of that information.

The Commissioner's report, *An Examination of BC Government's Privacy Breach Management* reviewed the policies, audit procedures and training within government as well as more than 300 privacy breach reviews completed by government's central breach management agency.

Between 2010 and 2013, 3,779 suspected privacy breaches were reported by government ministries, agencies and service providers to the Office of the Chief Information Officer. The majority of suspected breaches (68%) were classified as "administrative errors," such as sending personal information to the wrong account holder, email address or fax number. Other types of breaches included unauthorized disclosure (16%), inappropriate access (4%), lost paper or electronic records (4%) and cyber-attacks or phishing (<1%).

The Commissioner's report found that under government's current practices, suspected privacy breaches are investigated promptly and advice is provided on preventative measures.

“Government’s centralized model for managing privacy breaches is a solid foundation, but what is needed now is a commitment to making improvements. With the number of privacy breaches on the rise, I expect government to be actively scanning for breach trends across government, bringing clarity to their privacy risk evaluation processes, and auditing privacy safeguards to ensure privacy and data security standards are met as well as public reporting to inform citizens.

“Most privacy breaches are preventable, but only if organizations take the opportunity to learn from their mistakes and implement lasting preventative strategies,” said Denham.

This report makes five recommendations that, if adopted, will help government enhance the efficacy of its breach management programme and build trust among citizens. The Commissioner will be following up with government in three months to gauge implementation of the recommendations. The Commissioner will continue examinations of breach management practices in the broader public sector in 2015.

An Examination of BC Government’s Privacy Breach Management is available for download at: www.oipc.bc.ca/report/special-reports

For more information about Data Privacy Day, visit www.staysafeonline.org/data-privacy-day/

Media Contact:
Michelle Mitchell
Communications Officer
250-217-7872
mmitchell@oipc.bc.ca