

## Contego Spotlight

Well you've seen all the press coverage by now. The Toronto Star – "Laptop theft highlights security issues"; CBC News – "Private data of 8,600 Ont. teachers compromised"; The Globe & Mail – "Private records of 8,600 Ontario teachers stolen". Just in case you haven't, here's the story from Canadian Press.

Toronto — the Canadian Press Published on Thursday, Jan. 28, 2010 6:17AM EST

Laptops containing sensitive and unencrypted records belonging to about 8,600 Ontario teachers have reportedly been stolen. CBC News says three laptops containing teachers' names, addresses and social insurance numbers were stolen from the Waterloo, Ont., offices of the Ontario Teachers Insurance Plan on Dec. 3rd. Most of the teachers work at elementary schools for the Toronto District School Board, who were informed of the theft last week. The thieves also broke into a cafeteria cash register in a theft Waterloo Regional Police characterize as a routine "smash and grab." This theft comes a month after a health worker in Whitby, Ont., lost a USB key containing the names and OHIP numbers of 80,000 people in Durham Region. This prompted Ontario's privacy commissioner to order government agencies to encrypt personal information on devices such as USB keys and laptops.

This is the nightmare we're all trying to avoid – so why does this story keep occurring?

The angle I'm hearing the most right now regards the fact that the personal files in question were left unencrypted on the stolen computers. I am certain that we will all be hearing from security vendors and resellers how their technology solution would have prevented this problem. There is no doubt that encryption solutions would have aided in reducing the risk that has been exposed here. There are also end point security management solutions that will very effectively remediate this problem. If you have the budget – technology can help you help you out of this. But wait. The big question that remains is not why these files were left unencrypted on these laptops. What must be asked is why sensitive information was being stored in any form on laptops in the first place.

If sensitive information is securely stored in a centralized location, the only information assets stolen in this situation would be three easily replaceable laptops. Please let's all learn from these events. Through the creation and enforcement of security policies we may all be able to keep these stories from happening. Before we spend another dime on more security, can we all please take a moment to review just exactly what it is we're trying to protect and determine how best to accomplish that goal. So, where is your organization's sensitive information being stored? How is it accessed? Are individuals who are entitled to access this information aware of their role and responsibility in keeping this information safe?

Let's all try to keep out of the news shall we.

Will Raeside