ALBERTA
OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

Report of an investigation into a missing USB Memory Stick

July 27, 2011

Edmonton Public School District No. 7

Investigation Report F2012-IR-01

(Investigations F5702, F5762, F5796 and F5860)

I. INTRODUCTION

[1] On March 29, 2011, the Edmonton Public School District No. 7 (the "School District") notified the Information and Privacy Commissioner ("the Commissioner") that a USB memory stick ("the USB Stick") was lost on March 23, 2011 somewhere in the secure areas of the Centre for Education ("the Building"). The School District informed the Commissioner that the USB Stick was not password protected or encrypted and contained the personal information of over 7,000 individuals.

[2] In response to the notification, the Commissioner initiated an investigation on his own motion under section 53(1)(a) of the *Freedom of Information and Protection of Privacy Act* ("the FOIP Act"). Section 53(1)(a) authorizes the Commissioner to conduct investigations to ensure compliance with any provision of the FOIP Act.

[3] Subsequently, the Commissioner received three separate complaints from individuals. The first complaint was received on May 4, 2011; the second complaint on May 30, 2011; and the third on July 8, 2011. The Complainants raised concerns to the Commissioner because their personal information was contained on the missing USB Stick.

[4] Under section 65(3) of the FOIP Act, a person who believes that their own personal information has been collected, used or disclosed by a public body in contravention of Part 2 of the FOIP Act may ask the Commissioner to review the matter. A right to ask for a review under section 65(3) can give rise to an inquiry. So that the Complainants may exercise their rights under section 65(3) of the FOIP Act, the Commissioner opened a separate case for each Complainant. Case F5762 was opened in response to the first complaint; Case F5796 was opened in response to the second complaint; and Case F5860 was opened in response to the third complaint.

[5] The Commissioner authorized me to investigate and try to settle any matter that is the subject of these complaints. As the subject matter of the complaints and the Commissioner's investigation is the same, I have prepared one investigation report concerning these matters.

II. ISSUES

[6] In summary, the issues for our Office are:

Issue #1 - Did the School District disclose personal information in contravention of Part 2 of the FOIP Act?

Issue #2 – Did the School District make reasonable security arrangements to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction as required by section 38 of the FOIP Act?

III. GENERAL

[7] The School District's employee files are kept in a digital format on the School District's secure network. Paper documents to be placed on employee files ("the Source Documents") are scanned as images onto the hard-drive of a computer. The images are then converted into PDFs and the PDFs are loaded onto the digital employee files. Two computers are used on a daily basis to scan the Source Documents. The scanning of the Source Documents is split between the two computers (referred to hereinafter as "Computer1" and "Computer2").

[8] The scanned images remain on the hard-drives of Computer1 and Computer2 until they are deleted by the School District. At the time of the incident, it was the School District's practice to delete the scanned images one year after they had been scanned.

IV. THE INCIDENT

[9] On March 21, 2011, Computer1 stopped working and needed to be re-imaged. Computer1's hard-drive contained the images of Source Documents that had been scanned from January 1, 2010 until March 21, 2011.

[10] When re-imaging a hard-drive, all data is lost from the hard-drive. So that the data would not be lost, an employee of the School District ("Tech1") copied the data from Computer1's hard-drive onto the USB Stick and then re-imaged Computer1. The USB Stick was then stored in a locked cabinet in a secure area of the Building.

[11] On March 23, 2011, another employee of the School District ("Tech2") was provided the USB Stick so that Tech2 could restore the data to Computer1. The School District said Tech2 recalls placing the USB Stick in his/her pants' pocket. In summary, Tech2 then traveled within the restricted areas of the Building, used the employee elevator, and entered a washroom on the 4th floor. Two hours later, Tech2 discovered that the USB Stick was missing.

[12] During the two-hour period before the USB Stick was discovered missing, there was a 'lock-down drill' in the Building. During the 'lock-down drill' employees were required to stay in a secure location, and no visitors were in the building.

[13] The School District said "*…this was an unusual situation. District practice is not to store data on local hard drive(s). Data is normally saved on the secure local network. However, in this situation the scanning process requires that the data is stored on a local drive. The staff members were in problem-solving mode, trying to resolve issues with the hard drive and scanner to get the scanning process back in operation. A decision was made to temporarily move the data to a USB stick so that the hard drive could be re-imaged. The entire scenario was exceptional.*"

V. THE SCHOOL DISTRICT'S RESPONSE TO THE INCIDENT

[14] In summary, the School District responded to the incident as follows:

[15] An immediate and ongoing search was conducted for the missing USB Stick. This search included retracing Tech2's steps; checking with specific employees, building operations and custodial staff; and, sending notices by email with a picture of the USB Stick to all employees in the Building and to nearby schools whose students may have been in the atrium of the Building.

[16] On March 28, 2011, after failing to locate the USB Stick, the School District took steps to determine what information was on the device. On March, 29, 2011, after determining the scope of the breach and the sensitivity of the information, the School District notified the Commissioner's office about the incident.

[17] From March 28, 2011 to April 5, 2011, employees in the School District's Human Resources Division ("HR") reviewed the Source Documents and the PDFs contained in the digital employee files to identify the types of personal information at risk for each affected individual.

[18] The School District sent initial notification letters to affected individuals from March 31, 2011 to April 4, 2011. A follow-up letter describing the actual type of personal information contained on the USB Stick was sent on April 8, 2011. The follow-up letter included: a description of the types of personal information pertaining to the individual, contact information for additional information, and an apology from the School District. The School District also informed the individuals that they could contact the Commissioner's office if they had concerns.

[19] In addition, the School District created a "Questions and Answers" document about the loss, and made this available to all employees of the School District.

[20] The School District says that, as of May 24, 2011, the total cost of the breach was $46,000. This includes staff time, overtime, supplies, postage, and other miscellaneous expenses.

VI. INFORMATION AT ISSUE

[21] The information at issue is the "personal information" contained on the USB Stick.

[22] The USB Stick contains a copy of the Source Documents that had been scanned onto the hard-drive of Computer1 from January 1, 2010 to March 21, 2011. The types of documents include, but are not limited to:

> Employment applications, resumes, transcripts, completed direct deposit forms (including cheques), copies of identity verification (i.e. driver's licenses, first page of passports, birth certificates, etc.), injury forms, payroll correspondence, pension correspondence, benefits forms and correspondence, education credentials (i.e. certificate, degree, diploma etc.), job information history, pay-benefits history, performance evaluations, police criminal records check reports, etc.

[23] Section 1(n) of the FOIP Act defines "personal information" as *"recorded information about an identifiable individual"* and includes, among other things; an individual's name, address, phone number, social insurance number (SIN), birthdate (DOB), and information about the individual's educational, financial, employment, or criminal history.

[24] The School District says the total number of individuals whose personal information is on the USB Stick is 7,662. The School District says that for 4,836 of these individuals there was minimal personal information on the USB Stick (i.e. demographic information, employee ID number). However, for 2,826 individuals, the images on the USB Stick *"included considerable personal information, including social insurance numbers, banking information or both."*

[25] The School District confirmed to our office that all three of the Complainants' personal information is contained on the memory stick.

VII. ISSUE #1 – DID THE SCHOOL DISTRICT DISCLOSE PERSONAL INFORMATION IN CONTRAVENTION OF PART 2 OF THE FOIP ACT?

[26] As the USB stick containing personal information was lost, there is a real risk of disclosure. However, there has been no evidence before our Office that the information has indeed been accessed by an unauthorized party. Consequently, I cannot find that there has been an actual disclosure of the Complainants' personal information at this time.

VIII. ISSUE #2 – DID THE SCHOOL DISTRICT MAKE REASONABLE SECURITY ARRANGEMENTS TO PROTECT THE PERSONAL INFORMAITON FROM UNAUTHORIZED ACCESS, COLLECTION, USE, DISCLOSURE OR DESTRUCTION AS REQUIRED BY SECTION 38 OF THE FOIP ACT?

Section 38 of the FOIP Act

[27] Section 38 of the FOIP Act places a duty on public bodies to make reasonable security arrangements to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction.

[28] "Unauthorized access" to personal information includes *"Situations in which information is stored in an unsecured manner such that someone can obtain unauthorized access"* (Order 98-002 [136])[1]. Unauthorized disclosure" means disclosing personal information in ways other than those allowed under section 40 of the FOIP Act (Order 98-002 [197]).

[29] The question of whether a public body has met its duty to protect personal information is based on reasonableness. A public body that has not made reasonable security arrangements will be in contravention of the FOIP Act, whether or not an incident occurs. However, reasonable "does not mean perfect"[2]. A public body that has made reasonable security arrangements may be found to be in compliance with the FOIP Act, even when a breach occurs.

---

[1] Our office's orders and investigation reports mentioned in this letter are available on our website at www.oipc.ab.ca

[2] Investigation Report F06-01, Office of the Information and Privacy Commissioner, British Columbia, available online at www.oipc.bc.ca

Analysis of the School District's security measures

[30] The sensitivity of the personal information on the USB Stick is high due to the types and volume of personal information involved (e.g. names, signatures, bank account information, SIN, DOB, copies of identity documents, etc.). Saving sensitive personal information to a portable device creates a significant risk of potential harm to affected individuals if the information was accessed or collected by an unauthorized party. The high sensitivity of the personal information coupled with the risks (saved to a portable device) required a proportionately high obligation on the part of the School District to protect it.

[31] The School District had policies and guidelines in place that if followed, would have protected the personal information contained on the USB Stick. For example:

- *Refrain from loading personal information on PIDs [Personal Information Devices] unless it is impossible to carry out their duties without this information";*
- *Maintain an inventory or copy of the personal information that is required for the specific tasks;*
- *If personal information must be placed on a PID, then that information must be password protected and encrypted*
- *Ensure the portable device is labeled with appropriate contact information in case of loss*

[32] However, the policies and guidelines were not followed in this case.

[33] The School District also provided FOIP training to its employees. For example, all new employees are required to attend a New Orientation Session which includes a segment on the Protection of Privacy. Other employees can attend optional FOIP Training. In 2008-2009 all employees in HR were required to attend customized FOIP Training for HR.

[34] The School District's policies and training are measures to protect personal information that should be continued. A public body is held responsible for the actions of its employees (see our Investigation Report 2001-IR-008 [29]). However, policies and training alone are not enough to provide reasonable security arrangements.

[35] I confirm that the Building has strong security features – the doors to offices and work areas are locked, including doors to stairwells. Visitors must sign-in with security. Visitors are able to access the atrium on the main floor of the building; however, they cannot travel elsewhere in the building unless they are escorted. The School District believes that the USB Stick was lost somewhere within the secure area of the Building. However, the School District also acknowledges that there is a *"…remote possibility that the USB stick is in the possession of someone external to the District…"*

[36] A USB Stick is a portable device. The fact that the USB Stick was used to transport sensitive personal information within the Building is not a reasonable security arrangement. Furthermore, the USB stick was not encrypted or password protected.

[37] The School District said the information contained on the USB Stick is not searchable by personal identifiers (such as names) and several layers of folders must be opened before a single scanned document can be accessed. As such, it *"would require effort to use for fraudulent purposes."*

[38] I acknowledge it may require effort to view the scanned documents. However, all of the scanned documents can be accessed, read, saved, copied, sent in an electronic format, printed, etc. Therefore, it is my view that the amount of effort required to access the information contained in the USB Stick is not sufficient to provide reasonable protection against the risk of fraudulent use.

[39] In addition, there were 15-months of scanned images on the hard-drive of Computer1. Retaining personal information for longer than necessary creates a security risk. If there had been only one month of scanned images on the hard-drive (as is now the School District's practice) there would have been significantly less personal information at risk on the USB Stick.

My findings of whether the School District made reasonable security arrangements as required by section 38 of the FOIP Act

[40] In this case, an excessive amount of personal information was contained on the hard-drive of Computer1. The personal information was copied onto the USB Stick that was not password protected, encrypted, and no inventory was made of its contents. The location of the USB Stick is unknown.

[41] As such, I find that the School District failed to protect the personal information as required by section 38 of the FOIP Act.

IX. RECOMMENDATIONS

Steps taken by the School District after the incident

[42] The School District has taken (and plans to take) a number of steps to address this incident and to prevent a similar recurrence, I note the following in particular:

- Scanned images will only be kept for one month after the PDF has been loaded into the employee file. All previously scanned images older than one month have already been deleted from Computer1 and Computer2. HR is continuing to review the scanning process to determine whether scanned images can be kept for an even shorter period of time. In addition, a new audit process has been developed to 'spot check' whether the scanned images are retained only for the minimum time necessary.

- All hardware (i.e. laptops, USB sticks, hard drives, etc.) in HR containing personal information must have the Director's approval before being removed from HR.

- HR employees have been reminded that portable electronic devices containing personal information must be encrypted, and where needed - HR employees have been issued encrypted USB sticks.

- All HR employees were reminded to safeguard personal information and HR intends to schedule FOIP refresher training for the 2011/12 school year.

- The School District's relevant policies and regulations were reviewed with employees in the Technology Department. In addition, processes, procedures and training have been reviewed by the Technology Department managers.

- The New Staff Orientation presentations (which are mandatory for new staff) relating to FOIP have been reviewed and updated. In addition, every year optional FOIP training is set up for the School District employees.

- District Records and FOIP Management together with HR and District Technology will be submitting recommendations arising from this incident for the Superintendent's consideration. These include a recommendation that all Decision Units that scan records containing personal information of students or employees be deleted weekly after processing, including all batched images.

[43] The School District has also contracted an external professional consulting firm to assess the District's overall approach to information security management and related practices.

Recommendations

[44] For the most part, I believe the above steps demonstrate reasonable security arrangements. However, in addition to these, I have one recommendation to the School District as follows:

[45] I recommend that the School District review the personal information it collects for the purpose of the employee files to ensure that the collection is authorized under section 33 of the FOIP Act and to report back to this office on this matter.

[46] Collecting excessive personal information creates a security risk. Public bodies should take reasonable steps to ensure they only collect the personal information that is required and necessary for purposes permitted by section 33 of the FOIP Act.

[47] The School District has confirmed to our Office that it accepts my recommendation.

VII. CLOSING REMARKS

[48] I have completed my review of this matter. I found that the School District contravened section 38 of the FOIP Act when it did not make reasonable security arrangements to protect the personal information contained on the USB Stick.

[49] I believe the School District has taken (and intends to take) reasonable steps to address the incident and to prevent a similar recurrence. I also note that the School District has accepted my recommendation as mentioned in this report. I have no additional recommendations to the School District.

[50] The costs of this incident, both monetary and otherwise, serve as a reminder to the School District and to other public bodies of the importance of collecting only the personal information that is required and necessary, retaining that information for only as long as is necessary, and protecting that personal information while you have it.

Submitted by

Veronica Chodak
Portfolio Officer, FOIP