September 17, 2008 **P-2008-003**

NEWFOUNDLAND AND LABRADOR

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

REPORT P-2008-003

Eastern School District

Summary: On 2 April 2008 Eastern School District ("ESD") contacted this Office to advise that three desktop computers had been stolen from an elementary school. One of these computers was the school server. Information on the server consisted of personal information including the names, addresses, MCP numbers, contact and bussing information of 83 school children. The Commissioner was contacted by ESD and asked to investigate. The Commissioner found that given the circumstances of this case, reasonable security measures were in place prior to the theft, in keeping with the obligations imposed by section 36 of the *Access to Information and Protection of Privacy Act* (the "*ATIPPA*"). Section 39 of the *ATIPPA* had also not been breached, given the difficulty associated with accessing the personal information, the speed with which the thieves had been apprehended and the fact that the server had been stripped. Since the theft, ESD has taken several steps to increase security arrangements and the Commissioner was satisfied that ESD had now implemented a multi-layered approach to protect personal information stored on the server, in keeping with its duty under section 36 of the *ATIPPA*. The Commissioner made no recommendations.

Statutes Cited: *Access to Information and Protection of Privacy Act*, S.N.L. 2002 c. A-1.1, as am., ss. 36 and 39.

Authorities Cited: Newfoundland and Labrador OIPC Report P-2008-002.

Other Resources: *Key Steps When Responding to a Privacy Breach*, ATIPP Office, Department of Justice, Government of Newfoundland and Labrador http://www.justice.gov.nl.ca/just/civil/atipp/ .

I BACKGROUND

[1] On 2 April 2008 this Office was contacted by officials from Eastern School District ("ESD") who notified us that a break and enter had occurred at an elementary school, and three desktop computers had been stolen. One of the stolen computers was the school server, which contained the information of 83 students, including student names, MCP numbers, addresses, grade levels, phone numbers and names of parents/guardians. It is this computer that is at issue in this Report. ESD asked this Office to carry out an investigation with respect to whether there had been a privacy breach.

[2] As noted in Report P-2008-002, this type of information is routinely collected by schools and is necessary for record keeping purposes, safety and legal purposes, as well as for planning and policy purposes. I also noted in Report P-2008-002 the reasons for collection of MCP numbers, and why this is not a recommended practice. Therefore, there is no need to explore this issue again in this Report.

II DISCUSSION

Response to Breach and Security Measures in Place

[3] According to the Department of Justice ATIPP Office document entitled "Key Steps When Responding to a Privacy Breach," it is clear that ESD correctly identified and applied the appropriate framework within which to approach this situation. The steps, as outlined in this document are as follows:

- Contain the breach
- Evaluate the risks
- Notification
- Prevention.

[4] With respect to containing the breach, this was not fully possible until the computer containing the server was recovered. Fortunately, this happened rather quickly. The RCMP were immediately notified of the break, enter and theft and suspects were apprehended the following day. Officials at ESD have advised that it does not appear that any data was accessed. They make this assessment considering the speed with which the police apprehended suspects and the fact the server was "stripped apart" and thus not in a usable state when recovered.

[5] Further, ESD advises that domain password authentication was present on all computers involved and would prompt for a username and password when the system was powered on and the operating system invoked. Then, in order to access personal information, the WinSchool database would have to be accessed. According to ESD, this entails the following process:

> … …
>
> *2. WinSchool server module started (runs as a server application only, no direct data access by users is possible via server application)*
>
> *3. Access to the WinSchool client software needs to be gained, and then this software needs to be installed on a workstation. Specific knowledge of how to install and configure the client software for this WinSchool system is required (this is not common knowledge)*
>
> *4. A user name and password for this WinSchool system database would have to be known*
>
> *5. Knowledge of how to use the WinSchool system is required (not common knowledge – not an intuitive system)*
>
> *None of the above process is automatic but would require much manual effort.*
>
> *Specialized knowledge and tools would have to be used to process the steps outlined above. This would make access to the database information a difficult process.*

Aside from the passwords described above, no other technical security features were installed on the computers.

[6] The second step in responding to a privacy breach is to evaluate the risks, including: the type of personal information involved; the cause and extent of the breach; the individuals affected by

the breach; and foreseeable harm resulting from the breach. This is necessary in order to determine what other steps are immediately necessary and what precautions should be taken in order to minimize, as much as possible, the chance of another breach occurring.

[7] The server was housed in a locked server room which was located inside a locked computer laboratory. The thieves broke a window to gain access into the school and then broke several internal doors to access the computers. Information on the server consisted of the personal information of 83 students, their parents, guardians and emergency contacts, including student names, addresses, phone numbers, dates of birth, MCP numbers, schools, grades, parents'/guardians' name and contact information and bussing data. As noted in Report P-2008-002, this information could be used for illicit purposes in the hands of the wrong person. Due to the small size of the school, the number of people affected was relatively small.

[8] As noted in Report P-2008-002, the third step in responding to a privacy breach is notification and this is directly related to the above evaluation of the risks. This analysis assists in determining whether notification is necessary, and if so, how it should be done and what information it should contain. The more sensitive the information, the more important the notification and the manner in which it is done becomes. Once people are aware of the breach and what information was potentially or actually exposed, they, along with the public body, can take appropriate steps to mitigate any potential risks associated with the information being disclosed.

[9] I believe that ESD acted appropriately in notifying the parents or guardians of all the children whose personal information was contained on the computer. It is also my opinion that ESD chose effective means (news release and letters sent home with all children) to do so.

[10] The fourth step in responding to a privacy breach is prevention. The cause of the breach must be thoroughly investigated, and safeguards and policies must be created or updated and implemented to minimize, as much as possible, the risk of another breach occurring. In this case, the cause of the breach was a break and entry resulting in the theft of the computers, one of which was the school server containing personal information.

[11] It is not possible to determine, with absolute certainty, whether the information contained on the computer was accessed. It is ESD's position that the information stored on the server was likely not accessed. They attribute this to the fact that the thieves were apprehended quickly (the next day) and apparently rendered the server unusable. Also, the database runs as a server-only application and therefore, no direct access to information via this computer is possible. The server can only be accessed through the WinSchool program which would have to be installed on a computer and then appropriately configured. This installation requires specialized knowledge and, in addition, a username and password is then needed in order to access the database.

[12] In response to this break-in, ESD conducted a security assessment throughout the district to review security provisions in place at all schools. Security aspects evaluated included both physical and technical security deployments. As part of the security assessment, all computer systems that store personal/confidential information were identified and configured with a power-on password, a BIOS locking supervisor password and a hard disk drive password. A power-on password is required as soon as the system is powered on, before access to general operating system functions is permitted and even before the BIOS (basic input/output system that determines what a computer can do without accessing programs from a disk) can be accessed, thus prohibiting potential tampering with BIOS settings. The BIOS password prevents the computer from fully booting unless the correct password is provided, and the hard disk drive password prevents the drive from retrieving data unless the correct password is provided.

[13] Further, a security system has now been installed at the school and several measures were taken to increase the security of the server room. The door has been replaced with a solid wood door, and the walls of the room have been extended to the ceiling, thus completely enclosing the room. Further, two borrowed light windows located in the server room wall have been removed and filled with wooden studs and gyprock to match existing walls. The window used to gain entry into the school and the door to the computer laboratory were broken by the thieves and have also been replaced.

[14] In addition to the measures taken as a result of the security assessment, several directives with respect to strong passwords, network administration and securing servers in schools were

also sent to all District schools. These policies mandate that servers be stored in a secure location at all times, with a limited number of people having access to them (maximum of two essential designated people in smaller schools and three in large schools), that the number of network administrators in schools be limited, that the sharing of network administrator account passwords is forbidden, and that strong passwords be used for the WinSchool application. Strong passwords are characterized by a combination of upper and lower case letters, numbers and punctuation characters. They are at least 8 alphanumeric characters long, are not a word in any language and are not based on personal information.

Sufficiency of New Security Measures - Requirements under the *ATIPPA*

[15] In order to determine whether there has been a privacy breach, I must look to the provisions of Part IV of the *ATIPPA*. In the present case, we are concerned with sections 36 and 39.

[16] Section 36 of the *ATIPPA* states as follows:

> *36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

[17] As discussed in Report P-2008-002, what amounts to "reasonable security arrangements" will vary depending on the circumstances and reasonableness must be measured on an objective basis. An assessment of the reasonableness of security measures includes an assessment of the foreseeability of the privacy breach, the seriousness of potential harm (discussed above), the cost of preventative measures and relevant standards of practice.

Foreseeability of the Privacy Breach

[18] While theft of desktop computers is certainly not impossible, and therefore not completely unforeseeable, it requires much more effort than the theft of a laptop computer. A desktop computer is much more cumbersome to transport, and is obviously not carried around by its user. If such equipment is going to be stolen, it cannot be done so inconspicuously, and will likely not be the result of a "crime of opportunity." Therefore, the risk of theft is somewhat reduced, and

the foreseeability of a privacy breach in this manner is also reduced. In this case, the server is housed behind several locked doors inside a locked school.

[19] Further, the information on the server is not readily accessible. In order to access the information, another application had to be obtained, installed and configured. This would require specialized knowledge, and even after the application was installed, a username and password would be needed to access the database. Finally, one would need some knowledge of how to use the program. This leads me to the conclusion that, given all the circumstances, a breach was not foreseeable.

Seriousness of Potential Harm – discussed above

Cost of Preventative Measures

[20] The cost of preventative measures is relatively minimal, and essentially involves locked doors, a security system perhaps and some form of technical security on the computer itself. The server is kept in a locked room and, after hours, the computer lab and the school are also locked. A security system has now been installed at the school and ESD has increased the security of the room in which the server is housed by completely enclosing it, removing the windows, and installing a solid wood door.

[21] As noted, the computers are password protected and power-on, BIOS locking supervisor and hard disk drive passwords have now been installed on all computers containing personal or confidential information. This increases the difficulty of accessing the information contained on these computers. Bypassing these passwords could involve physically dismantling or tampering with the hard drive of the computer.

[22] With respect to administrative security, as briefly described above, ESD has put policies in place to restrict access to personal information. Notification to staff of the existence of these policies occurs via “e-mail conferences” in the ESD e-mail system. These conferences are accessible to all school principals and serve as bulletin boards for announcements and directives

to schools. The e-mail system has a feature which allows for tracking access to the various postings. This is a useful feature indeed, as policies and directives are of no use if staff is unaware of their existence.

Relevant Standards of Practice

[23] With respect to relevant standards of practice, there appears to be a lack of case law or other relevant authority on general guidelines for securing personal information stored on desktop computers. Each case is different and therefore, what is reasonable in each case is also different. Obviously, limiting access to such computers is one way to reduce the likelihood of a breach. While such a policy was lacking prior to the theft, ESD has now implemented one. Also, strong passwords seem to me to be a basic security measure. While strong passwords were not mandated prior to the theft, they are now. Also of importance is that in this case, ready access to the personal information was not possible. This, combined with the fact that the computer was housed in a secure location, minimizes the likelihood of a privacy breach, even in the absence of additional technical security measures. Nevertheless, ESD has now installed three layers of password protection on all computers used to store personal information. However, I would like to caution that every case is different and depending on the circumstances, additional security measures may be necessary. This is something that must be assessed on a case by case basis.

[24] Given the particular circumstances of this case, I am satisfied that ESD had reasonable physical security arrangements in place prior to the theft, despite the fact that administrative and technical safeguards may seem to have been somewhat lacking. It is important to remember that in this case, direct access to the information contained on the server was not possible. Access to additional software and knowledge of how to install, configure and use it as well as access to a username and password for the database would all be necessary before information on the server could be accessed. Therefore, I find that no breach of section 36 has occurred.

[25] Further, ESD has now taken additional steps to increase security measures to protect personal information. They have increased the physical security of the server room, installed a security system, installed three layers of password protection on all computers containing personal

information and have also implemented several directives with respect to personal information protection. I am quite satisfied with ESD's efforts and believe that ESD has now successfully implemented a multi-layered approach to information protection.

[26] As mentioned previously, we must also consider Section 39, which states as follows:

> *39. (1)A public body may disclose personal information only*
>
> *(a) in accordance with Parts II and III;*
>
> *(b) where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;*
>
> *(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 40 ;*
>
> *(d) for the purpose of complying with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province or Canada ;*
>
> *(e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information;*
>
> *(f) to an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;*
>
> *(g) to the Attorney General for use in civil proceedings involving the government;*
>
> *(h) for the purpose of enforcing a legal right the government of the province or a public body has against a person;*
>
> *(i) for the purpose of*
>
> *(i) collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body, or*
>
> *(ii) making a payment owing by the government of the province or by a public body to the individual the information is about;*

(j) to the Auditor General or another person or body prescribed in the regulations for audit purposes;

(k) to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem;

(l) to a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;

(m) to the Provincial Archives of Newfoundland and Labrador , or the archives of a public body, for archival purposes;

(n) to a public body or a law enforcement agency in Canada to assist in an investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result;

(o) where the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada , or

(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;

(p) where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is mailed to the last known address of the individual the information is about;

(q) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted;

(r) in accordance with an Act of the province or Canada that authorizes or requires the disclosure; or

(s) in accordance with sections 41 and 42 .

(2) The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.

[27] As described above, the thieves were apprehended the day following the theft. Further, the server had been stripped and gaining access to the personal information contained on the server would have been difficult. Although these factors do not guarantee that an unauthorized user never accessed the information, in the absence of any evidence to the contrary, I am persuaded, on a balance of probabilities, that there has not been a disclosure of personal information contrary to section 39 of the *ATIPPA.*

III CONCLUSION

[28] I have found that given the circumstances of this case, the security measures in place prior to the breach were reasonable. Therefore, there was no breach of section 36 of the *ATIPPA.* As I am persuaded that the information contained on the server was not accessed, I also find that there was no breach of section 39.

[29] In Report P-2008-002, I determined that, given current standards, a multi-layered approach to information security was necessary. With the improvements made to security since the theft, ESD has successfully implemented such an approach. Technical, administrative and physical security have all been increased, thus meeting the obligation under section 36 of the *ATIPPA*.

[30] As there was no breach in this case, and ESD has taken appropriate steps to implement a multi-layered approach to information security, I have no recommendations to make.

[31] Dated at St. John's, in the Province of Newfoundland and Labrador, this 17th day of September, 2008.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador