ALBERTA
OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

Report on an investigation into personal information discovered on a purchased computer server

July 4, 2013

Bow Valley College

(Investigation F6436)

(Complaint Investigations: F6527, F6528, F6530, F6531, F6533, F6546, F6547, F6553, F6557, F6561, F6562, F6563, F6576, F6577, F6578, F6581, F6584, F6598, F6600, F6608, F6609, F6610 F6632, F6633, F6637, F6654, F6812, and F6836)

Investigation Report F2013-IR-01

I. INTRODUCTION

[1] On September 19, 2012, an individual informed the Information and Privacy Commissioner (Commissioner) that he had purchased a used computer server from a computer wholesaler. He purchased the server in the spring of 2012 but did not turn on the server until September 2012. When he booted up the server, he found databases containing the personal information of thousands of Bow Valley College (BVC) students and employees.

[2] The Commissioner decided to initiate an investigation into this matter on her own motion under section 53(1)(a) of the *Freedom of Information and Protection of Privacy Act* (FOIP Act). Section 53(1)(a) allows the Commissioner to conduct investigations to ensure compliance with any provision of the FOIP Act. Notification was sent to BVC on September 21, 2012.

[3] In response to the Commissioner's notification, BVC conducted its own investigation into this matter. BVC informed our Office the server was one of twenty-one (21) decommissioned servers that the Electronic Recycling Association of Alberta (ERA) had picked up from BVC on May 1, 2012. ERA subsequently sold the server to a computer wholesaler. BVC said its investigation found that eight of the 21 servers (including the one purchased by the individual from the computer wholesaler) still had personal information on their hard disc drives.

[4] BVC retrieved the server from the individual, reviewed its contents and found the personal information of approximately 183,900 students and 3,500 employees, and notified the affected individuals.

[5] Under section 65(3) of the FOIP Act, a person who believes that their own personal information has been collected, used, or disclosed in contravention of Part 2 of the FOIP Act may ask the Commissioner to review that matter. From November 26, 2012 to January 1, 2013, the Commissioner received twenty-eight (28) separate complaints against BVC from affected individuals. All the Complainants expressed concern that their personal information was still on BVC's former server.

[6] The Commissioner authorized me to investigate this matter. As the subject matter of the Commissioner's investigation and the complaints is the same, I have prepared one investigation report to set out my findings and recommendations.

[7] The Commissioner also authorized me to investigate ERA's activities in relation to this matter under the *Personal Information Protection of Privacy Act* (PIPA). I will issue a separate investigation report in relation to the activities of ERA.

II. INVESTIGATION APPROACH

[8] For the purpose of my investigation, I spoke with the individual who purchased the server, BVC's representatives, ERA's representative, and several of the Complainants. I also reviewed all of the information provided to this Office by the individual, the Complainants, BVC and ERA. BVC also provided me written confirmation that the personal information of all 28 Complainants was indeed contained on the recovered server.

III. ISSUES

[9] The issues for my investigation are:

1. Did BVC make reasonable security arrangements to protect personal information?

2. Did BVC disclose personal information in contravention of Part 2 of the FOIP Act?

IV. INFORMATION AT ISSUE

[10] Personal information is defined under section 1(n) of the FOIP Act as *"recorded information about an identifiable individual, including…"*, and would include (among other things) an individual's name, address, social insurance number (SIN), date of birth (DOB), an identifying number assigned to the individual and information about the individual's educational history.

[11] As stated earlier, ERA had picked up 21 decommissioned servers from BVC on May 1, 2012. Of these 21 servers, BVC found that 8 (including the one purchased by the individual) still retained personal information.

[12] BVC said the eight servers were used as "test servers" not "production servers". They contain "testing information" made up of the real data copied from BVC's databases and fake data. The purchased server had copies of all of the data from all of BVC's data bases. The remaining seven servers had some of the data from some of BVC's database. As a result, each of the remaining seven servers had some of the same personal information that was on the purchased server.

[13] BVC said personal information of approximately 183,900 students and 3,500 employees over a nineteen year period (from 1991 to 2010) was on the purchased server. The personal information varied by individual, and included: names, email addresses, home addresses, phone number(s), DOB, SIN, BVC ID numbers, Alberta Education Student numbers, credit card numbers with expiry dates, salary, etc.

[14] BVC made arrangements for me to review the information and I confirm that "personal information" is contained on the purchased server.

V. INVESTIGATION FINDINGS AND ANALYSIS

Did BVC make reasonable security arrangements to protect personal information?

The duty to protect personal information

[15] Section 38 of the FOIP Act places a duty on a public body to make reasonable security arrangements to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction. The question of whether a public body has met this duty is based on reasonableness.

Details provided to this Office by BVC

[16] BVC said it contracted ERA to wipe the data from the decommissioned servers. As evidence of its contract, BVC said it is a member of ERA and according to ERA's website the services provided to members include:

- Pickup services of unwanted and disposed of equipment
- Data wiping, on or off site, with RCMP or DOD Certified Software
- Physical destruction of hard drives, servers, and other electronic devices
- Consulting services

[17] BVC also stated that prior to obtaining a membership they toured ERA's facilities and determined that their data destruction services were adequate for BVC's purposes. BVC stated that *"ERA has always purported to the College that data destruction would occur on all computers and servers provided to them prior to ERA disposing of the electronics through either a re-sale or recycling."*

Details provided to this Office by ERA

[18] ERA is a non-profit society whose mission is to reduce electronic waste through the reuse and recycling of unwanted computers, laptops, and other related electronic equipment. Items picked up by ERA are sorted into those that are reusable and those that are not. ERA donates some items. ERA also sells some items (like a case lot of computers) to a wholesaler. The wholesaler resells these items.

[19] ERA said the payment of a membership fee is a donation. Members still pay for ERA's services, such as pick-up services and data wiping services. ERA provided this Office with copies of their actual invoices showing separate charges for pickup and data wiping services. ERA also said that BVC has not had a valid membership for a few years now.

[20] ERA confirmed that BVC requested a pick-up service and ERA picked up the decommissioned servers on May 1, 2012. ERA said BVC did not request data wiping services, or tell ERA that there was data on the equipment. ERA's May 1, 2012 invoice to BVC is for pick-up charges only, and does not include any charges for data wiping.

[21] ERA said it does have formal written agreements with clients to provide data wiping and other specified services. ERA provided this Office with a copy of its template for its "Service Agreement". However, ERA also said that they have no formal agreements in place with BVC, *"and we have never guaranteed any services to them, in writing or otherwise…"*

My Analysis and Findings about BVC's protection of the personal information

[22] The sensitivity of the personal information on BVC's decommissioned testing servers (particularly the purchased server) is high due to:

- The types of personal information (name, DOB, SIN, ID numbers, home addresses, phone numbers, emails, charge card numbers and dates, etc.);
- The volume of personal information (the entire contents of BVC's databases for a 19-year period); and,
- The number of affected individuals (approximately 183,900 students and 3,500 employees).

[23] A public body cannot contract out of the FOIP Act (see Orders[1] 2000-003 [26] and 2000-029 [54]). As such, BVC (not ERA) is accountable under the FOIP Act for making reasonable security arrangements to protect the personal information on its decommissioned servers.

[24] Our Office has consistently urged organizations to implement three layers of protection: physical, administrative and technical/electronic (e.g. PIPA Advisory 8: Implementing Reasonable Safeguards[2]", and Investigation Reports P2006-IR-005, H2006-IR-002, H2007-IR-002). While these requirements have been raised in investigations conducted under the *Personal Information Protection Act* (PIPA) and the *Health Information Act* (HIA) these requirements are also relevant to public bodies subject to the FOIP Act.

[25] *PIPA Advisory 8-Implementing Reasonable Safeguards* provides the following guidance on reasonable safeguards that would be relevant to the circumstances of this investigation:

> **Technical Safeguards…**Completely delete or wipe all personal information no longer required for legal or business purposes from computer storage devices (diskettes, tapes, CD-ROMs, hard drives). If wiping is not possible, physically destroy the devices…
> …
> **Contracting** Contracts between organizations and third party service providers should include provisions for ensuring appropriate information management and security practices by the third party (e.g. contractors, consultants, support service providers, etc.).
>
> - Third parties should not have access to personal information without a signed contract/agreement in place.
> - Contracts should limit the third party's collection, use and disclosure of personal information to what is required to provide the contracted service.
> - Third parties should be required to:
>   - meet or exceed the organizations' security standards
>   - have staff sign confidentiality (non-disclosure) agreements
>   - report information security breaches to the organization
>   - have disaster recovery and system backup protocols in place
>   - return personal information at the end of the contract
>   - retain personal information according to the organization's records retention policy, or destroy it only as authorized by the organization

[1] Orders mentioned in this Investigation Report are available on our website at www.oipc.ab.ca.
[2] Accessed on June 26, 2013 at http://oipc.ab.ca/Content_Files/Files/Publications/PIPA_Advisory_8_Reasonable_Safeguards2007.pdf

- Contracts/agreements should include provisions allowing for the organization to audit/monitor the third party's compliance with contract provisions.

[26] BVC believed it had contracted ERA to wipe the data from the computer servers. However, BVC had no signed contract or agreement in place with ERA. In addition, although BVC was charged for "pick-up" it received no invoice for data wiping charges, or certificates to confirm that the data was wiped, or written assurance that the devices were physically destroyed.

[27] Consequently, I find that BVC did not make reasonable security arrangements to protect the personal information as required by section 38 of the FOIP Act.

Issue #2 – Did BVC disclose personal information in contravention of the FOIP Act?

[28] Section 40(1) of the FOIP Act allows a public body to disclose personal information only under certain circumstances. If section 40(1) does not authorize the disclosure, then the disclosure is in contravention of the FOIP Act.

[29] BVC confirmed to me that each Complainant's personal information was contained on the purchased server. The individual who purchased the server also told me he was able to view the personal information on it, and described specific elements of personal information, including names. In addition, I viewed some of the personal information that was contained on the copy of the purchased server.

[30] As such, I conclude that BVC's failure to protect the personal information resulted in an unauthorized disclosure of personal information in contravention of Part 2 of the FOIP Act.

VII. RECOMMENDATIONS

BVC's response to the Incident

[31] BVC took a number of steps to respond to this matter, including the following:

- Immediately ceased using a third party in the decommissioning of its servers.
- Recovered the purchased server directly from the individual who purchased it.
- Reviewed its inventories to identify all of the decommissioned servers with personal information that ERA picked up from BVC on May 1, 2012.
- Contacted ERA to try to determine what happened and whether the other seven decommissioned testing servers had been wiped. BVC assumes that the remaining severs were destroyed.
- Reviewed the contents of the purchased server to identify the affected individuals. For the remaining seven decommissioned testing servers that were not recovered, BVC determined that the same individuals were affected with the same personal information. As a result, BVC decided to send one notification to the affected individuals about this matter.

- Notified the affected individuals through a variety of means including: face-to-face meetings, publishing information on BVC's website, sending emails, sending 160,000 letters, setting up an information call line and email for questions. BVC received approximately 1,400 calls and 1,800 emails concerning this matter.

- Apologized to the affected individuals and advised them of their right to make a complaint to the Commissioner's office.

- BVC completed its own investigation to determine what happened.

- BVC told this Office that it had costs of over $247,900.00 to respond to this incident.

[32] During an April 18, 2013 meeting with me, BVC's representatives stated that they have now put procedures into place that include an onsite wipe process. BVC will no longer rely on a third party for the wiping of its equipment except for a second wipe. BVC's IT expert will check to ensure that information is properly wiped before equipment leaves BVC.

[33] BVC's representatives also stated that the data used in the test environment will no longer be saved onto the hard disc drives of testing servers.

My Recommendations

[34] I believe BVC took reasonable steps to respond to this matter. I also believe the above measures demonstrate reasonable security arrangements.

[35] As such, I have no further recommendations to BVC in relation to the decommissioning of its computer servers. However, I would encourage BVC to review its retention and disposition policies to ensure that it retains personal information only for as long as is necessary for legal and business purposes, and that personal information is disposed of in a reasonably secure manner.

VIII. CLOSING REMARKS

[36] I have completed my investigation into this matter. In my opinion, BVC contravened section 38 of the FOIP Act by failing to implement reasonable security arrangements to protect the personal information on its decommissioned computer servers. I also find that this failure resulted in the unauthorized disclosure of personal information.

[37] However, I believe BVC has taken reasonable steps to address this matter and has made reasonable arrangements to prevent a similar recurrence. I also note that BVC has apologized to the affected individuals. As such, I have no additional recommendations to BVC concerning this matter.

[38] Lastly, in my opinion, I believe this investigation settles this matter as I see no practical remedy that could be offered to the Complainants if they wish to proceed to inquiry on this matter under the FOIP Act.

Submitted by,

Veronica Chodak
Portfolio Officer