EYES WIDE SHUT: THE BEST DEFENCE IS A GOOD OFFENCE

By: Catherine Korte, Partner, McCague Borlack LLP

With the increasing interconnectivity of businesses to date, information is now exposed to a broad number of threats. Businesses need to ensure there is protection of information in order to prevent loss, unauthorized access or misuse. Businesses must have in place a process of assessing threats and risks to information and the procedures and controls to preserve the information. There are three guiding principles:

1. Confidentiality. Access to data must be limited to authorized parties.

2. Integrity. The data must be authentic and complete.

3. Availability. The data must be accessible, as needed, by those who are authorized to access it.

(Foundations of Information Privacy and Data Protection; A Survey of Global Concepts, Laws and Practices; Peter Swire, Kenesa Ahmad).

To minimize the risk to an information system, many factors need to be considered. One industry standard risk assessment formula is: Risk = Threat x Vulnerability x Expected Loss.

Security metrics help evaluate the effectiveness of security policies, processes and products as well as calculate the risk and determine the value of reducing or mitigating a risk. Some of the metrics that contribute to a risk/threat/vulnerability/loss matrix are the number of security breaches, the number of system outages and the number of lost information assets. Additional factors include the presence of software viruses and the use of investigation such as computer auditing and forensics.

The PC World Work Life Productivity recently published the 10 best practices to prevent data and privacy breaches as follows:

Data breach resulting from poor networking choices. Small and medium businesses often generally lack the budget necessary for equipment foregoing the use of routers and plugging directly into the Internet.

1. Data breach resulting from improper shredding practices. The "dumpster diving" identity thieves target businesses that throw out paperwork without shredding it. All documents with sensitive information or personally identifiable data need to be thoroughly shredded before disposal.

2. Tax records theft around tax time. Businesses need to be focused on incoming and outgoing information related to taxes. Identity theft often steal tax returns from an outbox or mailbox.

3. Identity theft resulting from public databases. Businesses publish information about themselves in public databases. Business owners will want to maximize its exposure while still protecting individual privacy. Many individuals with Facebook profiles have their address and date of birth. Many identity thefts can use information searchable publicly to construct a complete identity.

4. Identity theft resulting from using a personal name. Sole proprietors that do not take the time to file a business as application are far higher risk of identity theft due to the personal name rather than the business names being published publicly.

5. Bank fraud due to gap in protection or monitoring. Business owners note that it is vital to balance their accounts every month to ensure cheques are not being written out of business funds. Businesses rarely, if ever, check what credit accounts have been opened under the business name. Monitoring services can alert business owners when new credit accounts are opened fraudulently.

6. Poor emailing standards. Many businesses use e-mail as if it is a secure means of communicating sensitive or confidential information. The reality is pretty much the exact opposite. Emails are available for a number of people other than the recipient, and there is generally ample opportunity for e-mail communications to be intercepted in transit. It is more appropriate to treat e-mails as postcards rather than sealed letters.

7. Failing to choose a secure password. Use secure passwords.

8. Not securing new computers or hard drives. Often businesses without a dedicated IT Department or security administrator should consider using outside consultants to lock down PCs and hardware. Larger businesses should insure IT Departments and their information security administrator secure all new computers and hard drives.

9. Social engineering. Social engineers are individuals that call and claim they are from another organization. Social networks like Facebook and Linked In. An attacker may even claim to be with a firm that the business owner does business with. If someone you do not know calls

on the phone, or contacts you by email through a social network make sure it is the person you think it is before revealing passwords and confidential information.

10. The Treasury Board of Canada has guidelines for privacy breach. The guidelines for privacy breach provide guidance to institutions on the management of privacy breaches. These deal with general requirements under the Act with respect to collection, retention, use, disclosure and disposition of personal information.

1. What is a privacy breach?

According to the Treasury Board of Canada website it involves the improper or unauthorized collection, use, disclosure, retention or disposal of personal information. A privacy breach may occur within an institution or off site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information sharing agreements or intruders.

2. Potential causes of privacy breaches

According to the Treasury Board of Canada Secretariat's website, these include the following situations that could result in the disclosure of, or access to, personal information by unauthorized parties:

- The theft, loss or disappearance of equipment or devices containing personal information;
- The sale or disposal of equipment or devices containing personal information without purging prior to sale or disposal;
- The transfer of equipment or devices without adequate security measures;
- The use of equipment or devices to transport or store personal information outside the office for telework or off-site work arrangements without adequate security measures;
- The inappropriate use of electronic devices to transmit personal information, including telecommunication devices;
- Intrusions that result in unauthorized access to personal information held in office buildings, file storage containers, computer applications, systems, or other equipment and devices;
- Low level of privacy awareness among employees, contractors or other third parties that handle personal information;

- Inadequate security and access controls for information in print or electronic format, on site or off-site;

- The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information;

- Insufficient measures to control access and editing rights to personal information, which may result in wrongful access to, and the possible tampering with, records containing personal information;

- Phishing or the use of deceptive tactics to trick an individual into providing their personal information either directly or by going to a fake website. For example, an individual pretending to perform system maintenance calls a government employee to obtain his or her security password; and

- Pharming or the use of a fake copy of an official Government of Canada website to redirect to a malicious web site in order to steal information without the user's knowledge. This method takes advantage of the weaknesses in the Data Network System (DNS). For example, an individual accesses what he or she believes is an official government website and submits personal information as requested by the site. The individual is unaware that he or she has been redirected to a fake copy of the official website.

3. Preventing privacy breaches

To prevent a privacy breach the Treasury Board of Canada has recommended institutions should:

- Follow the requirements of the Policy on Government Security (PGS) and other security direction issued by the Treasury Board of Canada Secretariat (TBS). The Royal Canadian Mounted Police (RCMP) and the Communications Security Establishment Canada (CSEC) also issue direction on physical and information technology security, respectively;

- Conduct Privacy Impact Assessments (PIAs) and Threat and Risk Assessments (TRAs) in accordance with the Directive on Privacy Impact Assessment;

- Take privacy into account before making contracting decisions or entering into information-sharing agreements. Government institutions should include adequate privacy protection provisions, such as a requirement to immediately notify the government institution of a privacy breach. For more information, consult the TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions;

- Provide regular and ongoing training to employees, managers and executives to ensure that they are aware of the requirements of the Code of Fair Information Practices, Privacy Act, related TBS policies, and departmental or agency security and privacy practices and procedures;

- Ensure that personnel working off-site are aware of their privacy and security responsibilities. This means ensuring that appropriate measures are taken to safeguard the personal information they handle off-site. Government institutions should consider keeping personal information in-house when telework or similar arrangements would involve considerable privacy risks (e.g., a large volume of personal information or sensitive personal data);

- Establish clear administrative controls that restrict access and editing rights to records containing personal information to only those employees who have a legitimate need to know, and for institutions to put in place appropriate audit trails to ensure that these administrative controls are functioning as intended;

- Use cryptography (encryption) to protect sensitive personal information stored in a computer or a portable storage device or being transmitted through e-mail, on a government network, a wireless network, or across the Internet. The PGS provides further direction on encryption;

- Purge all equipment and other electronic devices containing personal information before selling, disposing of, or transferring such equipment or devices;

- Empty security containers such as file cabinets, safes or mobile shelving units and ensure that no classified or protected material is left inside before selling or transferring them to other responsibility centres or outside the government;

- Take precautions against "phishing" and "pharming":

    - Ensure that requests for personal information are valid and that individuals asking for personal information are who they claim to be;

    - Refuse to provide personal information in response to an unsolicited telephone call, fax, letter, email attachment or Internet advertisement;

    - Be on the lookout for clues indicating that a website may be fraudulent (e.g., spelling errors, unusual advertisements, or portions of the site that do not work properly);

    - Check the lock icon at the bottom of your browser to ensure that you are sending personal information over a secure connection; and

- Verify the phone number and call the organization to determine validity if you have any concerns.

4. Privacy Breach Management Process

Institutions should consult the Privacy Breach Management Toolkit for effective privacy practices, plans and procedures to address privacy breaches.

Examples of best practices in managing privacy breaches include:

- Preliminary assessment and containment;
- Full assessment;
- Notification (to affected individuals and internal management where required);
- Mitigation and prevention;
- Notification of the Office of the Privacy Commissioner of Canada (OPC) and the TBS; and
- Sharing of lessons learned.

In summary, the best defence is using a good offence to prevent privacy breaches from occurring in the first place.