Interested in learning more about security?

SANS Institute InfoSec Reading Room

Act Now! An Introduction To Canada s PIPED Act and its Affect on Organizations and IT Departments

The Personal Information Protection and Electronic Documents Act (PIPEDA or PIPED Act) by the Canadian parliament, has received little media attention considering its scope. Stephanie Perrin, chief privacy officer for Zero-Knowledge Systems in Montreal notes "...the Canadian public doesn't know that the act has passed by and large." (Conrath). This paper has been written to cast some light on this important piece of legislation and the inherent responsibilities it imposes on organizations and IT departments. This paper...

Act Now! An Introduction To Canada's PIPED Act and its Affect on Organizations and IT Departments

GIAC Security Essentials Certification
Practical Assignment 1.4b
Option 1

Submitted by Kevin Egan
SANS ILOT (15 May 2002)

4 October 2002

Abstract

Rapid growth in technology has allowed near global access to an unrestricted on-line community. This is exciting and empowering, but vigilance is of paramount concern in order to protect the interests of the global community as our businesses, our governments, and we grow in this information age. To this end, global, public, and private sector initiatives are being undertaken to address the need to protect the privacy of individuals by introducing legislation, regulations, or guidelines governing the collection, use, and disclosure of personal information. One such initiative is the passing of the Personal Information Protection and Electronic Documents Act (PIPEDA or PIPED Act) by the Canadian parliament.

The PIPED Act has received little media attention considering its scope. Stephanie Perrin, chief privacy officer for Zero-Knowledge Systems in Montreal notes "...the Canadian public doesn't know that the act has passed by and large." (Conrath) This paper has been written to cast some light on this important piece of legislation and the inherent responsibilities it imposes on organizations and IT departments. This paper will begin with a list of some important global initiatives that protect personal information privacy and five commonalities they share. An introduction to Canada's privacy legislation will be followed by a summary of the 10 privacy protection principles introduced in the PIPED Act. Concluding this paper will be a discussion of six milestones that organizations and IT departments can use to mark their progression along the path to compliance, including guidance on implementing each.

Introduction

Advances in technology, specifically database technology, have permitted unprecedented ease in the ability to collect, correlate, and disseminate large quantities of information in a short amount of time. The power of today's desktop computers exceeds that of enterprise servers from only a short time ago. Seemingly innocuous collections of information from disparate sources can be correlated to create a database with remarkably detailed facts about an individual.

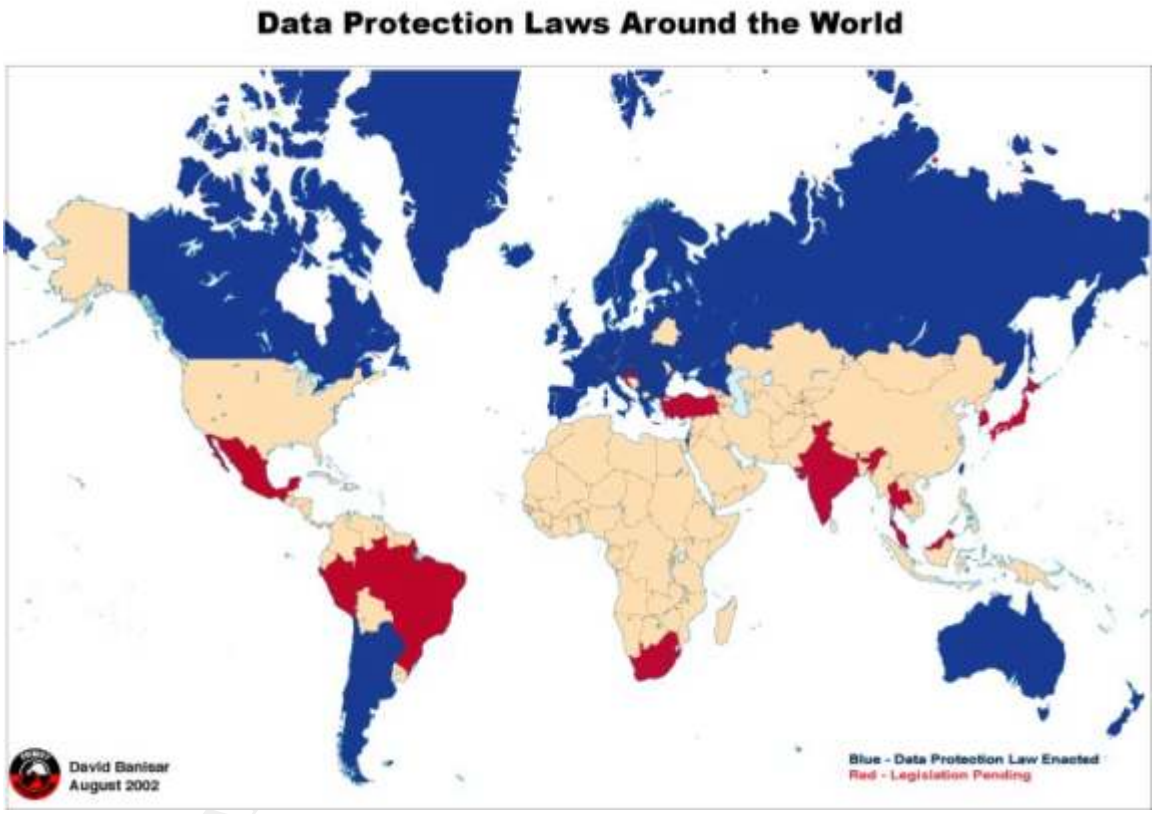
As electronic commerce becomes ever more pervasive and global events call for increased foreign and domestic security, outdated practices are being replaced by more current legislative or de facto regulations enforcing good information handling policies. These regulations impose responsibilities on organizations and IT departments to create or update administrative policies and security policies with provisions protecting personal information.

Overall, clarity in how an organization uses the personal information it collects fosters a healthy, open, and trusting relationship with customers, clients, and business partners. Customers who are confident in how an organization handles their personal information will continue to do business with them.

Global Initiatives Effecting Personal Privacy Protection

A number of global initiatives are in place to address the growing need and consumer demand for legislative or regulatory control, either in whole or part, over the collection, retention, use, and disclosure of personal information. Figure 1 (below), courtesy of David Banisar and Privacy International, illustrates those countries that have legislation or are enacting legislation to protect personal privacy:

Figure 1: World Data Protection Map



(Banisar)

Figure 2 (Page 5) shows several examples of privacy legislation initiatives including the title, country of origin, and purpose of the legislation:

Figure 2: Legislative Initiatives

Title	Country of Origin	Purpose
European Union Data Protection Directive of 1995 (EU Directive 95/46/EC)	European Union (EU) Member States	Protection of personal information.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	USA	Privacy protection for personal health information.[1]
Children's Online Policy Protect Act of 1998 (COPPA)	USA	Privacy protection for children using the Internet.
UK Data Protection Act of 1998	United Kingdom	Legislative principles behind the EU Directive 95/46/EC.
Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999	USA	Obligations placed on financial institutions to protect personal information.
Safe Harbor Framework of 2000	Agreement between the USA and the European Union (EU).	Simplify U.S. organizational compliance with the EU Directive.
Privacy Amendment (Private Sector) Act of 2000	Australia	Protection of personal information.
Personal Information Protection and Electronic Documents Act of 2000	Canada	Protection of personal information.
Bill to Protect Personal Data of 2001	Japan	Protection of personal information.
Model Data Protection Code for the Private Sector	Singapore	Protection of personal information.

In general, the personal information privacy goals these initiatives are designed to achieve can be summarized as follows:

1. Consent: Organizations must obtain consent whenever personal information is used.

[1] HIPAA stipulated a deadline for congress to enact the proposed Health and Human Services (HHS) regulations regarding the protection and confidentiality of healthcare information. Since this deadline was not met, HHS moved forward and updated the original proposed regulations in a final ruling that is to come into force on October 15, 2002.

2. Fair Collection: Personal information must be fairly collected and not collected under coercion or false pretences.
3. Informed and Limited Use: What the information will be used for must be clearly stated and is limited to the purpose for which it was collected.
4. Accessibility: Individuals must be provided access to their personal information and have means to correct, update, or remove it.
5. Security: Appropriate measures must be taken to protect personal information as it is stored or transmitted.

While the principal thrust of these documents is similar, the philosophy on implementation varies. Some believe that uniformly legislating these principles is the best method for enforcing them. Such countries include the United Kingdom, the European Union (EU) Member States, Japan, and Canada. The United States, however, takes a slightly different approach as outlined in the Safe Harbour Overview: "The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation." (Safe Harbour Overview) Singapore has a set of codes of conduct that, while not uniformly stated in legislation, embodies principles from many laws containing privacy and data protection provisions.

Canada's Privacy Legislation: An Introduction

Canada's private sector privacy legislation, the Personal Information Protection and Electronic Documents Act (also known as Bill C-6) was developed to support and establish Canada as a leader in electronic commerce initiatives. The PIPED Act not only addresses how personal information is collected and used, but also how transactions are electronically stored. It responds to global initiatives like that of the European Union, which directly influence the flow of information between European and other countries. On 14 January 2002 the EU officially recognized the PIPED Act. The honourable Pierre Pettigrew, Minister of International Trade, stated, "Canada is the first non-European country to be recognized as providing legislated privacy protection that meets the rigorous standards of the EU Directive." (Théberge)

In his guide entitled "Your Privacy Responsibilities", the Privacy Commissioner of Canada states, "the Act reflects the process of its creation, the hammering out of a consensus between business professionals, consumer advocates, and public policy experts." (Your Privacy Responsibilities) The PIPED Act is a unique and pioneering body of legislation in that it has been drafted based on national standards derived from the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (CAN/CSA-Q830-96) created in 1996.[2] Canada has the distinction of being the first country to establish a national standard to protect personal information privacy.

[2] The Model Data Protection Code for the Private Sector (created by the National Internet Advisory Committee – NIAC in Singapore) is based on the CSA Model Code as well.

The PIPED Act sets out the following important definitions:

> "Commercial activity" means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.
>
> "Federal work, undertaking or business" means any work, undertaking or business that is within the legislative authority of Parliament.
>
> "Organization" includes an association, a partnership, a person and a trade union.
>
> "Personal information" means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization. (PIPED Act. Section 2)

Cases that come before the Privacy Commissioner are handled based on the specific circumstances surrounding that case. For this reason the definition of personal information is intentionally broad and leaves room for interpretation. A more detailed definition is not required since most compliance issues will be resolved internally or through mediation rather than through judicial means. Some examples of personal information include name; age; social insurance number; driver's license and health card numbers; credit, loan, and bank records; medical information; social status; and criminal records.

The PIPED Act applies to organizations in the following three phases.

As of **1 January 2001** the PIPED Act applied to federally-regulated organizations including banks, telephone companies, shipping and air carriers; information about the employees of these organizations; and the transmission of personal information across provincial and national borders.

As of **1 January 2002** the PIPED Act additionally applied to personal health information used by these organizations. Personal health information includes information such as mental and physical health.

On **1 January 2004** the PIPED Act will apply to personal information use by all organizations in Canada unless the organization operates within a province that has similar legislation.[3]

[3] Quebec has such legislation. Other provinces such as Ontario, Manitoba, New Brunswick, and British Columbia are considering the creation of such legislation. The term used in the PIPED Act is *substantially similar* and refers to legislation that has been found to be at least as protective.

Part 1 of the PIPED Act, which is most relevant to this paper, sets out the rights of individuals to have their personal information protected. It also recognizes the need for businesses to collect, use, or disclose personal information during the course of day-to-day business. It outlines 10 standardized fair information practice principles derived from the CSA Model code (included as a schedule located at the end of the PIPED Act) that organizations must follow whenever personal information is used. These fair information practices are summarized in the next section.

The 10 Privacy Protection Principles

1. Accountability: Organizations must appoint a person responsible for compliance with the PIPED Act; publish documents and train staff on the practices developed to protect personal information; deal with queries and complaints; and ensure any third parties use comparable levels of protection when processing personal information.
2. Identifying Purpose: Organizations must identify the purpose of collection before the information is collected and must have permission to use the information if that purpose changes.
3. Consent: Organizations must have permission to collect, use, and disclose personal information and cannot coerce, deceive, or offer services conditional on consent.[4] Consent may be withdrawn.
4. Limit Collection: Organizations must only collect the necessary information to fulfill the purpose outlined in principle two.
5. Limit Use, Disclosure, and Retention: Organizations must use and disclose personal information only with consent and for the original purpose it was collected. Personal information should be kept only as long as necessary to fulfill the purpose.
6. Accuracy: Personal information must be accurate, complete, and up-to-date.
7. Safeguards: Organizations must ensure the confidentiality and integrity of personal information whether it is stored on paper or electronically.
8. Openness: Organizations must be open about their processes concerning personal information. It must be clear who is accountable for the organization's compliance, how individuals may access their personal information, and what types of information the organization collects. A copy of literature that explains these practices, and what information may be shared by the organization must be available.
9. Individual Access: Individuals must have access to their personal information and details on how it has been used. This is to be done in a reasonable timeframe and if possible, without cost.

[4] In cases where there is investigation of fraud or breach in law, the person is a minor, or seriously ill, consent may not be required. Limits to consent are outlined in Section 7 of the PIPED Act.

10. Challenge Compliance: The organization must provide a forum for addressing challenges to its compliance, must investigate and document all complaints, and if necessary, must update its practices.

The remaining sections of Part 1 of the PIPED Act detail specifics surrounding these principles and include additional definitions; limits to the collection, use, and disclosure of personal information based on reasonable expectation; methods of challenge resolution; a list of offences; and protection for whistleblowers who notify the Privacy Commissioner of violations.

Compliance Milestones

It is clear that the 10 fair information practice principles embodied in the PIPED Act impose significant responsibilities on organizations and their IT departments. Section 5 of the PIPED Act clearly states that organizations must comply with these 10 principles. The Privacy Commissioner of Canada has published a document (entitled, "Your Privacy Responsibilities: A Guide for Businesses and Organizations to Canada's Personal Information Protection and Electronic Documents Act".[5]) that provides complete and detailed information for organizations seeking compliance. The remainder of this paper will serve as a companion to this document and will elaborate on specific issues. Prior reading of "Your Privacy Responsibilities" is not required.

Regulations on all commercial organizations come into effect on 1 January 2004, which gives organizations approximately 15 months to become complaint. There is much to be done in this timeframe, especially for organizations that are thus far unfamiliar with the requirements, or even existence, of the PIPED Act. Organizations must begin implementing or upgrading their existing policies immediately.

Listed below are six milestones that organizations and their IT departments can use to mark their progression while implementing the 10 principles of privacy protection. Guidance on what types of information need to be included in the policies that address each principle is also included.

Milestone 1: Designate a privacy officer

Organizations must designate an individual or individuals who are familiar with the PIPED Act to be responsible for the organization's compliance. This person should also be familiar with the organization's current information handling practices. Selecting a backup individual will ensure that there is always a qualified person available to address the needs and concerns of customers, even if the primary person is unavailable.

[5] Your Privacy Responsibilities.

An adequate budget must be allocated to training an organization's privacy officer, senior management and staff. A general familiarity with the personal information practices and proper request handling practices of the organization is essential and will help ease the burden on those directly responsible. It is good business practice to keep members of the organization informed about issues of security and personal information handling; make this part of the organization's layered defence (defence-in-depth) strategy.

Milestone 2: Create a privacy statement

The next issue to tackle is creating the organization's privacy statement. If it already exists, the statement should be checked against the 10 privacy protection principles. Does it clearly identify who the person responsible for privacy issues is? Does it address issues concerning who, what, when, why, and how personal information is collected, used, and disclosed? Additionally, organizations should incorporate the following in their privacy statement:

- The organization's philosophy on personal information. This should indicate that the organization values and protects personal information provided by customers.
- Encouragement for questions and comments on the organization's practices. Feed this information back into policies during revision.
- Adequate contact information for the organization's privacy officer.
- Clarity and simplicity. It is critical to ensure that privacy statements and supporting policies are in plain language, are easy to understand, and are specific to the purpose for which the information is required. Avoid overly broad statements of purpose, complicated or technical language, and details. For example, stating that the organization uses a Cisco PIX firewall, Tripwire intrusion detection, and DESX encryption to protect files is unnecessary and overly technical. This would also provide valuable information and do much of the reconnaissance work for those who would use this information against the organization. The organization's guarantee of protection is only meaningful if it is understood. Simply state the organization's commitment to protecting personal information. The privacy officer may provide more information if an individual seeks greater detail.

Place the privacy statement in a clearly marked area on the organization's Website (Internet, Intranet, and Extranet if they exist) and in any publications (newsletters, brochures, etc.) that are released–whether internal or external. If such a statement did not already exist, consider drawing special attention to it once it has been created. This is now part of the corporate image and will instil trust and confidence in clients and business partners.

Milestone 3: Audit current information handling polices, procedures, and stores

If these policies exist, dust them off and review them to make sure they are consistent with the privacy statement set out in Milestone 2. It is essential that the organization's outward policy be reflected internally.

Even if the organization is without written policies and procedures regarding the handling of personal information, current practices will provide a wealth of information with which to get started.

Review steps taken when a new client is set up or when client information is requested or retained. Consider the following questions:

- Is there a form that is filled out when starting up a new file?
- What information is collected and is the purpose for collection clearly stated?
- Where and how is this information stored?
- Is everyone in the organization permitted access?
- How is access restricted?
- Is the organization protected by an alarm system and alarm monitoring or security company?
- Does the organization have a file room or filing cabinets where client information is stored?
- Is there a lock on the file room or cabinet door?
- Do workstations and servers use passwords or file systems that support access control lists (ACL's)?
- Does the organization have a firewall or an intrusion detection system (IDS)?
- Does the organization use encryption to store and transmit information?
- Does the organization share information with third parties and is the use of this information regulated? If so, how is it regulated?

Evaluate current information handling practices and take note of any shortcomings or additional practices that will be required for compliance. Armed with this data the organization can begin writing specific policies and procedures.

It is unnecessary to re-collect any information the organization already has. However, organizations are obligated to obtain consent in order to continue to use and disclose this information. As well, the organization must ensure it only retains information necessary to achieve the purpose for which it was originally collected. Perform an audit of personal information stores checking for information that does not conform to this purpose; make provisions for the safe removal of extraneous personal information. This audit process should be performed regularly to ensure that the organization remains compliant. If the purpose for collection changes, another audit will be necessary.

Milestone 4: Create specific policies and procedures to be followed in the handling of personal information

In the course of writing policies and procedures to incorporate the 10 principles, develop tools such as standardized templates and internal checklists that clearly indicate organizational practices and the responsibilities of individuals who are collecting, using, amending, de-personalizing, disclosing, sharing, or removing personal information. Create such templates for the fulfillment, tracking, and denial of requests for personal information and to track disagreements or complaints. Include specific guidelines for how the organization will handle a privacy breach incident.

For example, the organization could create an application form for information commonly collected from clients, customers, and business partners. This form should clearly state the information required by all 10 principles. Checkboxes can be used to provide clients with the ability to opt-in or opt-out of specific uses for their information. As well, include a list of common reasons the organization has for collecting information. Staff will quickly be able to check off the appropriate reason and the client is clearly made aware of why the information is being collected. Provide space for signatures so that the individual whose personal information is in question can show expressed consent. Expressed consent protects all parties involved.

Save and store these documents in a specific place to be used when needed. These records will also provide proof of the organization's processes and an audit trail if the organization's practices are ever audited or under review. Use of these tools will help streamline processes and reduce the additional overhead placed on day-to-day operations.

In addition to following the organization's guidelines for writing policy documents, include the intended purpose of the policy, any existing policies that are subordinate or cancelled by the new policy, the reason for its introduction, what it covers, who has responsibilities under it, the actions that need to be taken in order to comply with the policy, and when these actions need to be taken.

The following is an example of an information collection policy. It is modelled after policies developed by the SANS Security Policy Program and incorporates the policy features defined in the SANS GSEC courseware:

Information Collection Policy

1.0 Purpose

The Information Collection Policy is intended to help employees determine what information should be collected/given from/to individuals during the course of services provided by <Company Name>.

2.0 Related Documents

Information collected under this policy should be used in conjunction with the following policies:

Information Labelling/Handling Policy
Information Use and Disclosure Policy

3.0 Cancellation

This policy does not cancel any existing policies.

4.0 Scope

This policy applies to any information collected by any member of <Company Name> whether in verbal, written, or electronic form. Information may be collected from individuals, clients, and third party organizations that have entrusted <Company Name> with information under a non-disclosure agreement, service level agreement, or any other agreement pertaining to the information.

Information collected by <Company Name> can be classified as either public or personal information and shall be designated as:

- <Company Name> Public
- <Company Name> Personal
- <Company Name> Third Party Public
- <Company Name> Third Party Personal

Public information is information that has entered into the public realm by any means. Public information can be found in telephone directories, newspapers, periodicals, news media, census and electoral data, and other media and government registries.

Personal information is any information about an individual that does not include the name; telephone number; title, business address, or telephone number of an employee of an organization; or information that is considered to be public.

Personnel who are uncertain of how to properly designate a piece of information should consult the <Company Name> Privacy Officer for clarification. If there is any question as to the designation of information collected, the information will be treated as personal.

5.0 Policy

The following guidelines must be used in either the collection or the creation of a template for collection of:

5.1. Public Information (including information from third parties)

There are no specific guidelines for the collection of public information unless stipulated in a contractual, service-level, non-disclosure, or other such agreement.

5.2. Personal Information (including information from third parties)

5.2.1. The specific purpose for the collection must be clearly stated and documented.
5.2.2. Overly broad purposes are not permitted.
5.2.3. The purpose must be limited to what a reasonable person would expect under the circumstances.
5.2.4. The individual from whom the information is collected must be informed of the purpose. Where information is collected from a third party, the individual to whom the information applies must be informed of the purpose.
5.2.5. Obtain and document consent for use of the information.
5.2.6. Consult the <Company Name> Privacy Officer for guidance in areas that are unclear.

<Company Name> has created the following templates to be used for collecting information:

Public Information Collection Form
Personal Information Collection Form
Third Party Public Information Collection Form
Third Party Personal Information Collection Form

These guidelines and templates provide the necessary components for PIPEDA compliant collection of information. Where a new template is being created, the <Company Name> Privacy Officer must approve the template before it is used.

6.0 Responsibility

6.1. Enforcement

An employee found to have violated this policy may be subject to disciplinary action.

6.2. Review

The <Company Name> Privacy Officer must review any changes to this policy prior to introduction. The <Company Name> Privacy Officer must also review this policy and ensure that it is up-to-date as purposes and circumstances for collection change, or as necessary.

7.0 Revision History

Friday, September 27, 2002 – Policy created.

Milestone 5: Implement specific safeguards

Up until this point, procedural policy has been discussed. It is now time to write and implement security policies that specifically address the need to protect the confidentiality, integrity, and availability of personal information that the organization stores. There are three security areas that must be addressed and they are categorized in the PIPED Act under Section 5 Paragraph 4.7.3(a)-(c) as organizational, physical, and technological security measures. Management and IT personnel must work closely to ensure successful implementation of these three areas.

Organizational Security Measures

To address organizational security needs, consider using security clearances to limit access to sensitive personal information on a need-to-know basis. Use controls that are congruent to the sensitivity of the information that is stored to aid in the reduction of costs and overhead. For example, it is unnecessary to protect less sensitive personal information such as voter information, which in Canada includes names and addresses, by storing it in a biometrically access controlled room. However, this might be appropriate for more sensitive information such as physical and mental health information, financial information, or criminal records.

In addition, keep staff informed and aware of current security issues as well as the information protection policies and practices of the organization. This is essential for good organizational security and must be included in the organization's policies. A recent survey of IT managers and professionals found the following:

> 33 percent believe that employees in their organization often bypass their security system (i.e. leaving computers on, writing down passwords, etc.) because the system is too cumbersome. (Canada's ITX Survey 2002)

Attempting to keep the balance between security and usability has always been an issue for IT departments and staff. The most effective way to address this is through effective user education. Use the following user education methods:

- Hold frequent meetings with staff and discuss the importance of maintaining the confidentiality and integrity of the personal information the organization uses.
- Make management and staff aware of the risks and potential impact to the organization's reputation and the financial losses that could result from a breach of policy.
- Ensure employees are clear on policies and practices that are in place, any tools that have been created (templates, checklists, etc.) to aid in the administration of policies, and when to use such tools.
- Review and discuss the nature of inquiries or complaints made by clients; update policies and practices if a complaint reveals any shortcomings.

Physical Security Measures

Ensure that any implement used to store personal information, whether it is a computer system, storage cabinet, file folder, handheld device, cellular phone, etc., is protected with adequate physical security measures. Maintaining good physical security includes the following:

- Ensuring portable devices are always attended or locked up using security cables, pads, or enclosures.
- Storing information in locked rooms, cabinets, and offices that are monitored by alarm systems and monitoring companies.
- Storing information in a fireproof safe or room.
- Having restricted access control measures in place such as swipe cards, proximity keys, and biometric security.
- Storing extremely sensitive information in electronically shielded rooms.

These measures notwithstanding, physical security is most commonly compromised as a result of simple oversight. Unfortunately, it is common for doors and cabinets to be left open or unlocked, and for the alarm to not be set when the last employee leaves. Extra care must be taken to ensure that this does not occur. To help minimize such incidences, it may be necessary to include disciplinary provisions in employment agreements and security policies.

Technological Security Measures

Finally, address the technological security measures that the organization will use to protect personal information. Keep in mind the following points:

- Use appropriate security depending on the sensitivity of the information the organization holds.
- Use the principle of least privilege to restrict access to only those individuals that require the information and permit only the necessary access rights.
- Use the defence-in-depth approach by layering security measures in order to create a more secure environment for the storage of personal information.
- Supplement physical security with such technology as fingerprint, voice, facial, or retina recognition systems (biometric access controls).
- Protect the organization from outside attacks by using firewalls on the network perimeter. Firewalls placed on the internal network at the entry point to personal information stores will provide an additional layer of protection.
- Use network and host based intrusion detection systems to monitor servers that store personal information for unauthorized activity.
- Organizations with a smaller budget can still reap the benefits of firewall and IDS systems using low cost or free utilities available on the Internet. Such utilities include personal firewall products like Zone Alarm, Tiny Personal Firewall, Sygate Personal Firewall, the TIS firewall toolkit (FWTK), the IPFirewall code built into the Linux kernel, as well as Black Ice Defender, and Deerfield Personal Firewall, which also have intrusion detection capabilities. Psionic Technologies offers a gamut of protection utilities that monitor for authentication anomalies, port scans, and security log violations. The SNORT intrusion detection system is an open source IDS utility for both the Unix and Windows environments. It is freely available and can also be used for packet sniffing and logging. Built-in operating system utilities such as NETSTAT can be used to check for holes (open ports) on systems that may permit unwanted access. In conjunction with NETSTAT, the VISION utility for Windows platforms (part of Foundstone's free forensic tools) and the LSOF utility for Linux platforms can be used to map system processes to any open ports that may be found. These tools are also beneficial in baselining and auditing an organization's systems.
- Use strong passwords, smart cards, biometrics, or one-time passwords to limit entry to networks internally and from the outside (through dial-in or VPN access).
- Use groups, file system access control lists (ACL's), and standards based encryption to secure files stored on systems and to limit access to only those individuals that require it. Do not use proprietary encryption schemes as they often prove to be insecure. Use only standards based encryption like DES, RSA, AES, or ECC.
- Use VPN's for employees and business partners that require remote connection to the corporate network and ensure comparable measures are in place on their systems as well.

- Write the requirement for these measures into contracts, service level agreements, and non-disclosure agreements.

Most importantly, baseline networks, systems, and devices to gather in-depth information about the type of traffic that flows through the organization. Find trends such as listening ports, user access times, and running services. Perform regular audits and compare the results against the baseline information to reveal any irregularities that might indicate system compromise. Investigate any anomalies thoroughly and follow the organization's incident handling policies if an incident is discovered (if these policies exist).

Milestone 6: Make compliance known

Since the organization has made the necessary investment in becoming compliant with the PIPED Act, it is now time to make this information known to the public. Send a newsletter and have employees speak with clients during meetings, verbal, or written correspondence to see if clients are aware of these new regulations and their rights under them. If they are not, provide them with the literature that has been created. In any case, be proactive. As part of the openness principle, it is the organization's responsibility to inform customers of their rights and the organization's responsibilities.

Conclusion

Technology is an enabler and cannot be realistically faulted for invasions of privacy. It is people and their use of technology that perpetrate such abuses. Fortunately, technology, when properly leveraged and backed by legislative and regulatory principles, can be used to help mitigate the risks. The business community must see compliance as an opportunity rather than an imposition. Negative publicity resulting from a misuse of personal information can have an incalculable affect on an organization's reputation and bottom line.

The third and final phase of the PIPED Act's implementation is quickly approaching. Organizations must not wait until the last minute to begin the process of creating, amending, and implementing their policies to include the principles of consent, fair collection, limited use, accessibility, and security. The introduction of the PIPED Act imposes these privacy protection responsibilities on organizations and IT departments. However, the impact on organizations that practice common sense when handling personal information will find the transition to be a natural evolution of existing practices and is, in any event, motivation to put such practices into place. Doing so is more than just a matter of compliance; it is a matter of good business.

References

Banisar, David. “Global Map of Data Protection.” Privacy International. 27 September 2002. <http://www.privacyinternational.org/survey/dpmap.jpg>

“Bill C-6 (The Personal Information Protection and Electronic Documents Act).” The Canadian House of Commons. September 28, 2002. <http://www.parl.gc.ca/PDF/36/2/parlbus/chambus/house/bills/government/C-6_4.pdf>

“Canada’s ITX Survey 2002.” Athabasca University Centre for Innovative Management. 24 September 2002. <www.mba.athabascau.ca/titan/aucimwebsite.nsf/AllDoc/182FCB19467C65E687256BFE001C8E20/$File/ITX-2002.PDF>

Conrath, Chris. "Complying with PIPEDA." ComputerWorld Canada. 1 January 2002. ITworld.com 23 September 2002. <http://www.itworld.com/Man/2693/020129pipeda/index.html>

“Data Protection Act of 1998.” U.K. Information Commissioner. 27 September 2002. <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def3080256636004 5bf4d/87e9812eb170b250802568da0057505a/$FILE/Directive95_46_ec.rtf >

“Diet Begins Debate on Bill to Protect Personal Information.” 8 May 2002. Foreign Press Center / Japan. 27 September 2002. <http://www.fpcj.jp/e/shiryo/jb/0215.html>

“Directive on Personal Data Protection enters Into Effect.” Europa – The European Union On-Line. 27 September 2002. <http://europa.eu.int/comm/internal_market/en/dataprot/news/925.htm>

“Financial Services Modernization Act.” U.S. Senate Committee on Banking, Housing, and Urban Affairs. 27 September 2002. <http://www.senate.gov/~banking/conf/grmleach.htm>

“Health Insurance and Portability and Accountability Act of 1996.” Assistant Secretary for Planning and Evaluation . 27 September 2002. <http://aspe.hhs.gov/admnsimp/pl104191.htm>

Hiong, Goh Seow. “Data Protection & Privacy in Singapore.” 27 March 2001. Deputy Director Infocomm Development Authority of Singapore.” 27 September 2002. <http://www.pco.org.hk/misc/singapor/sld001.htm>

"Implementation Schedule." The Privacy Commissioner of Canada. September 28, 2002. <http://www.privcom.gc.ca/legislation/02_06_02a_e.asp>

"Model Data Protection Code." TrustSG. 28 September 2002. <http://www.trustsg.org.sg/pdf/Model%20Data%20Protection%20Code.pdf>

"New Rule Will Protect Privacy of Children Online." Federal Trade Commission. 27 September 2002. <http://www.ftc.gov/opa/1999/9910/childfinal.htm>

"NIAC Launches Two Major Initiatives to Address Concerns Over Data Protection and Undesirable Content on the Net." 5 February 2002. Singapore Broadcasting Authority. 28 September 2002. <http://www.sba.gov.sg/sba/detailed.jsp?artid=362&typeid=1&cid=0&bSubmitBy=true>

"Opinion 2/2001 on the Adequacy of the Canadian Personal Information and Electronic Documents Act." Article 29 – Data Protection Working Party. 27 September 2002. <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp39en.pdf>

"Privacy in Australia." The Office of the Federal Privacy Commissioner. 28 September 28, 2002. <http://www.privacy.gov.au/publications/pia1.html>

"Privacy Rule." U.S. Department of Health & Human Services. 27 September 2002. <http://www.hhs.gov/ocr/hipaa/privruletxt.txt>

Radwanski, George , The Privacy Commissioner of Canada. "Your Privacy Responsibilities." Office of the Privacy Commissioner of Canada. 22 September 2002. <http://www.privcom.gc.ca/information/guide_e.asp>

"Safe Harbor Overview." Export Portal, U.S. Department of Commerce. September 22, 2002. <http://www.export.gov/safeharbor/sh_overview.html>

"SANS Security Policy Project." The SANS Institute. 30 September 2002. <http://www.sans.org/newlook/resources/policies/policies.htm>

Théberge, Sébastien." European Commission Recognizes Canadian Legislated Privacy Protection." Industry Canada. September 14, 2002. Office of the Minister of International Trade. 22 September 2002. <http://www.ic.gc.ca/cmb/Welcomeic.nsf/261ce500dfcd7259852564820068dc6d/85256a220056c2a485256b3e0065e682!OpenDocument>

Uehara, Soichiro, and Shogo Asanuma. "Recent Trend in Personal Data Protection in Japan." Electronic Commerce Promotion Council of Japan (ECOM). 27 September 2002. <http://www.ecom.or.jp/ecom_e/home/research_file/20011119recenttrend.pdf>

Last Updated: July 27th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
Security Awareness Summit & Training 2017	OnlineTNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced