SYS-X

The Impact of the Personal Information Protection and Electronic Documents Act (2004)

The **Personal Information Protection and Electronic Documents Act** and Canadian Business

On January 1, 2004 The **Personal Information Protection and Electronic Documents Act (PIPEDA)** came into force in Canada. There is a good chance you have never heard of it, or if you have you do not think it applies to your business. There is also a good chance that you are wrong. This act has an impact on every Canadian business that collects and keeps personal information about individuals. This act applies equally to the local auto shop that keeps information on one hundred and fifty active clients and to the large multinational that keeps information about hundreds of thousands of current, past and potential clients. If your company keeps personal records of clients or suppliers, this act applies to you.

The Act

PIPEDA was created with one very clear goal in mind. To protect personal information from being misused. Over the last several years the incidents of **Identity Theft** have been on the increase. Add to this the amount of personal information that is being sold from one organization to another and the amount of unsolicited mail and e-mail this has caused the government felt it was time to act. You will need to get a copy of the actual act to see all of the details, but the act can broadly be broken into two main themes, **Protection of personal information** and **Access to personal information**.

Protection of personal information

Any organization that collects information about individuals must keep that information secure. This includes the physical security of the information itself as well as keeping people who should not have access to this information away from it. In most organizations very little control is exercised over where personal information is stored and in fact quite often no one within the organization can definitively say what kind of information is being kept about people and who has control of that information. Quite often many different departments within a single organization capture information about the same group of people independently. Not withstanding the security issues, this has historically lead to out of date information being in use by company officials even though someone within the company has obtained updated information from someone. It is very hard to protect something that no one can definitely say even exists. Under the act, organizations must be proactive to identify the information that they are keeping, why they are keeping it and who has access to and control of it.

Access to personal information

As well, every day a significant amount of e-mail is exchanged between people and organizations that contain information of a critical or personal nature. One out of every four emails sent today is scanned for content during transmission over the Internet. Some estimates say that by the year 2005 every email will be scanned at least twice. PIPEDA says that information owners must take responsibility for any personal information that is transmitted in an email that finds its way into the wrong hands. It appears that information owners are going to need to encrypt all email that they send or they will need to take steps to obtain specific authorization from people to communicate personal information by email and acknowledgment of risk this involves.

Any individual who believes that their personal information is being kept by an organization has the right to know what information is being kept, how it is being used and how to request that the information not be kept. Every organization must identify someone whose job it is to field these requests and properly respond to them. If someone calls your organization and asks for the person in charge of access to personal information, they must be given a contact. If they ask for the standards being used by the organization to keep information they must be given it. If they ask to be removed from your list they must be removed. The act provides for some exceptions to this rule, such as an employer can keep necessary information on an employee without their permission and a company who is owed money by an individual can keep information on that person. Obviously if someone does not want their information kept, that may impact on the ability of the company to provide services to this person and so they may well cease to be a client.

The Security Audit

The first thing every Canadian company should do, to ensure that they are in compliance with PIPEDA is to hold a security audit. The goal of the audit is to get control of the information that the company is keeping about individuals and to ensure that they are complying with all aspects of the act.

Step 1: **Identify a Personal Information Coordinator for the organization**. This person's role will be to keep track of the Personal Information that the organization keeps as well as to be the contact for inquires from the general public with respect to this information. Clearly for a small organization this Coordinator position will not be a full time job but for a large company this may in fact amount to an entire department of people.

Step 2: **Identify the information being kept.** This sounds horribly simple but the reality, as stated earlier, is that most companies, especially large ones, have no idea what information is being kept. Once this aspect of the audit has been completed the PI Coordinator should have an organized list of all of the areas within the organization that keep personal information, what information is being kept and who is using it for what. As well during this step it will be possible to identify instances where more than one group within an organization is keeping the same set of information about the same group of people. Clearly it will be advantageous to eliminate this duplication.

Step 3: **Identify a clear owner of the data and the People who need Access to this information.** The goal of this step is to identify the individuals who need access to each collection of information. Each collection of data should have a very clear owner who is in charge of ensuring that only people with a need to have access to the information have access. It is not necessarily enough to say that anyone who is an employee of an organization has access to all information captured by the organization. For each collection of data that an organization collects there should be a natural set of people who need to have access to it.

Step 4: **Identify the technology being used to store and protect the data.** This includes identifying the storage medium, flat files, paper records, database tables or even e-mail repositories. It also includes identifying the servers on which the data resides and the access that people both inside and outside of the organization have to these servers. Are the servers on internal networks, or are they in externally available networks or Demilitarized Zones (DMZs). Are there services running on these servers that make other information available to internal or external people, and does this put this information at risk?

Step 5: **Create Procedures and guidelines with respect to Information storage**. These procedures should include guidelines on everything from:

i. What kind of information is stored?
ii. What kind of information is definitely NOT stored ever?
iii. Who is information stored for and why?
iv. How do internal people start a new data repository?
v. How do internal people apply to get access to information, and what guidelines are used to approve or deny this access?
vi. How are pieces of hardware that may contain personal data disposed of?

vii. How do people get access to the information that is being stored?
viii. How do people request that information not be stored?

Step 6: **Investigate encrypted email solutions.** If an organization is exchanging email with people that contain information of a sensitive or personal nature, that organization should seriously consider mandating that all such electronic communication should be encrypted. This applies to email being exchanged between employees, employees and clients and employees and vendors. At a cost of less than $200 per user per year, this is the single most cost effective way to keep the information private and still permit email to be used.

Step 7: **Investigate User agreements.** Every person who is not an employee of the organization for whom information is being kept **must** be informed of that fact and must be asked for permission to keep the data. They must be informed of the policies that organization has with respect to personal data and they must be permitted to opt out. During this step information owners must identify whether suitable agreements are in place.

Step 8: **Create an Action Plan.** All of the analysis that has been done will identify issues that need to be dealt with. The final product of a complete security audit is an action plan that is to be followed to ensure all identified security issues are dealt with.

Step 9: **Revisit the audit at least annually.** Just because an organization has guidelines and procedures does not mean employees will follow them. On at least an annual basis, perhaps as often as monthly for large organizations, the Security audit should be done again. This can range from redoing the entire audit to randomly picking departments or groups within the organization to launch surprise audits on.

How Sys-X Corporation Can Help

Sys-X Corporation has been in the information business for a number of years. We have built and managed information repositories for large clients such as **Sony of Canada, Canada Life, MDS Sciex, Cedera, Dye&Durham** and **the government of Ontario.** We have also worked with a number of much smaller organizations like **Aegent, Ventext Corporation** and **William M. Mercer**. We are available to come in to an organization to assist with a security audit in any capacity that is required. We would be happy to come into an organization and provide a complete independent security audit or to come in and assist internal resources to perform the audit.

The Author

Sean Forbes is the owner of Sys-X Corporation and has over fifteen years of experience in the IT industry. Sean spent nine years working at IBM as a software developer before joining and eventually becoming CEO of Sys-X Corporation.

Sys-X Corporation is a Software Services Consulting, Development and Resources firm delivering full-service project or resource based solutions to a diverse set of private and public organizations.

Our focus and commitment is to provide smart, proactive services at high quality standards with partner-like support.

Our dedication to excellence and customer fulfillment provides the foundation for our capabilities in delivering solutions to clients in today's challenging environment.