
Why Privacy and Data Security Should Matter to Businesses

Industry Spotlight

www.ShapeYourVision.com

With large scale privacy breaches frequently making headlines within the last few years, there is a growing concern among individuals about information security and about the collection, use, disclosure and retention of their personal information by organizations. In May 2008, retail giant **TJX** which owns Winners and HomeSense in Canada compromised 45.7 million customer accounts. In January 2009, **Monster Worldwide Inc.**, a popular job site, compromised its users' accounts when its database was illegally accessed for the second time in two years. In July 2009, **Facebook**, the popular social networking site was found to be in violation of Canadian privacy law. Not surprisingly, the focus on security and privacy has largely been on large organizations that collect and retain large amounts of personal information.

With the growing number of small and medium enterprises (SMEs) in Canada, data security and privacy is an issue that all companies should be aware of. However, in March 2007, a survey¹ conducted on behalf of the Privacy Commissioner of Canada's Office found that SMEs have a low to medium awareness about their responsibilities under Canadian privacy laws; this has prompted a push to increase awareness about privacy in the SME sector.

To help raise awareness and to provide guidance in this sector, the Canadian Institute of Chartered Accountants (CICA) published a toolkit called "**The Canadian Privacy and Data Security Toolkit for Small and Medium Enterprises**" that features a foreword by the Privacy Commissioner of Canada. This comprehensive toolkit serves as a valuable resource for organizations who want to be proactive in identifying data security and privacy risks, and sends a clear message to SMEs that the cost to react to a data breach is much greater than the cost to develop and implement preventative measures.

Impact of Data Breaches on SMEs

According to **Nicholas Cheung, CA** and a **Principal in Assurance Services Development** at the **CICA** and contributing author of the Toolkit, SMEs tend to offer more personalized service than larger organizations so a privacy breach would likely be more damaging to their business relationship with customers. For example, "individuals will go to SMEs because they like the special and personal attention they get and often develop a stronger trust type of relationship with these companies. If an SME violates that trust by saying we have had a privacy breach, it tends to be more personal with the individuals," says Cheung.

Security Enables Privacy

Even though security can exist without privacy, privacy cannot exist without security. In other words, no matter what security measures companies put in place to protect their IT systems, it does not guarantee the privacy of individuals' personal information.

¹ Findings from a Survey of Canadian Businesses relating to privacy issues & the implementation of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, commissioned by the Office of the Privacy Commissioner of Canada, March 2007.

"If your employees aren't aware of how to protect that information using the IT systems and data security safeguards that you put into place, then it's all for not. Security is the enabler of privacy but privacy is about the complete picture of how to protect something including training and implementing proper privacy policies and procedures," explains Cheung.

Self-Assessments

With 56% of data security breaches occurring internally², companies can benefit by conducting security and privacy self-assessments to help them identify possible weaknesses in their privacy programs. For a quick analysis, the CICA's toolkit contains two self-assessments – one for security and one for privacy – and provides resources to deal with the weaknesses that companies may uncover.

For organizations requiring a more thorough assessment, companies can use the **Generally Accepted Privacy Principles (GAPP)**, a comprehensive framework that the CICA developed in conjunction with the American Institute of Certified Public Accountants. These internationally recognized privacy principles can be used to identify and assess privacy risks and can be used as the basis for a privacy audit. As of October 2009, revisions have been made to GAPP to include over 70 criteria and a multitude of best practices and controls that companies can adopt for their own privacy programs.

Once companies identify their weaknesses through the self-assessments, they can develop and revise their privacy policies and security programs according to their needs. Programs can range from simple to complex depending on the enterprise but companies should be knowledgeable about their own security posture and their privacy responsibilities under the law.

Information Access

Access restriction is necessary for information security and could limit the productivity of workers but companies need to review the access provided to their employees and contractors to ensure that the right people have the right access for what they need to do without compromising security or productivity. For example, "when employees leave a company, or when companies have frequent contractors or temporary workers, companies are exposed to a lot of [data] risks. Companies should make sure that these individuals' access is properly revoked on a timely basis," stresses Cheung.

Information Risk Management Practices

According to a 2008 study, 88% of data breaches are caused by insider negligence.³ Not surprisingly, many companies do not take the appropriate measures when it comes to information disposal. Employees will often unthinkingly throw sensitive documents into a recycling bin or the garbage and in some cases, mistakenly believe they have deleted sensitive electronic documents on their computers only to discover later that the information can still be accessed by unauthorized users. To minimize data threats, information should be securely disposed of through a cross-cut shredder where there is little chance of the documents being recreated, or put through an electronic shredding program if the information is in electronic format.

The same study also revealed that lost and stolen portable devices like laptops and USB keys account for 49% of data breaches. To minimize security threats, Cheung recommends that laptops' hard drives and USB keys be properly encrypted and not just password protected; that devices never be left unattended in plain view where they can be easily stolen; and that companies practice risk avoidance and question whether or not taking personal information offsite is actually required or not.

Despite two-thirds of companies reporting they do not train their employees in compliance with privacy legislation⁴, **training and awareness programs** are actually the number one preventative measure

²⁻³ 2008 Annual Survey: "Cost of a Data Breach", PGP Corporation and the Ponemon Institute, February 2009.

⁴ Findings from a Survey of Canadian Businesses relating to privacy issues & the implementation of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, commissioned by the Office of the Privacy Commissioner of Canada, March 2007.

undertaken by companies once a breach has occurred.⁵ In fact, companies that exercise information risk management practices actually reduce their data breach costs by approximately 16% over companies that do not.⁶ Based on these findings, companies can avoid the high costs associated with data breaches by investing in privacy training for their employees ahead of time.

Effective Information Security

In order for information security to be effective within an organization, companies should develop their own privacy policies, educate their employees about them and explain their privacy policies to their customers. According to Cheung, this is a good way for companies to demonstrate their commitment to their customers' privacy. He also encourages that companies have their employees sign off on **privacy and data security policies** to ensure that employees are aware of their obligation to customers and to their employers. By holding employees accountable and making them aware of the consequences of non-compliance, it encourages them to act in accordance with companies' expectations of data security and privacy. For example, "when I get issued a laptop, I understand what the company's expectations are in terms of protecting that particular device and for me to take the appropriate means to protect it and not to leave the laptop unattended in the front seat of my car," explains Cheung.

Privacy Laws

Currently, the federal **Personal Information Protection and Electronic Documents Act (PIPEDA)** does not protect the personal information of employees unless the enterprise is a federal work, undertaking or business; however, in some provincial jurisdictions employees are included in private sector privacy laws. To send a positive message to private sector employees and to afford them the same privacy protection as their customers, Cheung recommends that companies' privacy policies extend to employees' personal information as well.

While **mandatory breach notification** is currently only required under Ontario health law, there is a proposed amendment to federal law and recommendations for other provincial jurisdictions to follow suit. This will likely encourage SMEs to assess their privacy practices sooner rather than later because data breaches, mandatory breach notifications and unwanted publicity will undoubtedly be even more costly than the cost to develop and implement appropriate privacy policies and security programs to minimize data threats.

With the high costs of data breaches, companies need to be proactive rather than reactive when it comes to privacy. Security is necessary to ensure that personal information is not viewed by unauthorized users and requires thoughtful planning. Through security and privacy self-assessments, companies can identify and assess their needs and from there can develop appropriate privacy policies and security programs to ensure the protection of their customers' personal information and in some cases, their own employees'. By implementing risk management practices like the secure disposal of information; introducing company procedures to handle portable devices; using encryption technology to secure sensitive information; and providing privacy training to employees, companies will benefit in the long run with fewer data breaches, reduced expenses and more satisfied customers.

⁵⁻⁶ 2008 Annual Survey: "Cost of a Data Breach", PGP Corporation and the Ponemon Institute, February 2009.

About the Author:

Eleanor Kwan, CSP, is the CEO and Founder of **ShapeYourVision®**. Her company provides expertise in the area of sales and service through strategy consulting and professional skills training to help companies increase revenues and client satisfaction. For more information, visit www.ShapeYourVision.com.