Privacy and Boards of Directors:

What You Don't Know *Can* Hurt You

Information and Privacy
Commissioner of Ontario

Ann Cavoukian, Ph.D.
Commissioner
July 2007

This publication is an updated, enhanced version of a paper released in 2003 by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario. Dr. Cavoukian gratefully acknowledges the work of Professor Richard LeBlanc of the Schulich School of Business, York University, and Debra Grant of the IPC, in preparing the first report, and Catherine Thompson of the IPC for her work on this updated report.

Information and Privacy Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Table of Contents

Executive Summary

The Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D., prepared this paper to raise awareness among corporate boards of directors about privacy. As a director, you face increased responsibilities, which now include ensuring that customer personal information is handled with care. Recent high profile data breaches show what can happen if privacy is left as an afterthought. The central message of this paper is that you cannot afford risking the serious harm to customers from lost or stolen data, as well as the potential liability and loss of business resulting from a breach.

This paper explains the importance of creating a culture of privacy within your organization. *Fair information practices* are also explained. They are a set of commonly accepted principles that organizations should apply to personal information in order to protect privacy – and that also form the basis of laws and policies related to privacy. These practices relate to accountability, identifying purposes, consent, limiting various activity (such as collection, use, disclosure, and retention of personal information), accuracy, safeguards, openness, access, and challenging compliance.

From a business perspective, the failure to address privacy can harm your reputation, your organization's reputation, and business relationships. It can also seriously harm your customers, and lead to customer mistrust and deterioration in your organization's information asset quality. Moreover, it can lead to a loss in market share, unexpected costs, and a drop in stock prices.

To assist in better understanding the importance of addressing privacy, this paper outlines the business case for sound privacy practices. The paper argues that sound privacy practices will give your organization a more positive image and a significant edge over the competition. Also, business development into other jurisdictions with privacy laws can be facilitated. Products and services can be customized to meet customer needs and will enhance strategic decisions. Moreover, good privacy practices will enhance customer loyalty, and will ultimately save you time and money. Treating privacy as a strategic business differentiator creates a positive sum scenario where the interests of both your organization and your customers are advanced.

The paper outlines specific steps you should take, including a self-assessment, educating yourself regarding privacy, appointing a Chief Privacy Officer, making privacy an integral part of performance evaluations and compensation packages, executing regular privacy audits, and asking senior management the right questions about privacy.

Introduction

Today, corporate directors are faced with a wide array of responsibilities arising from their board membership. For example, the far-reaching *Sarbanes-Oxley Act* passed in 2002 significantly reformed corporate responsibility in the United States by introducing requirements aimed at improving the accuracy and reliability of corporate disclosures to investors. Directors also have a fiduciary duty to act in the best interests of the corporation and a duty to maintain an appropriate standard of care. In Canada, the statutory standard for the amount of care, diligence and skill required of directors is codified at section 134(1) of the *Ontario Business Corporations Act*[1] and section 122(1) of the *Canadian Business Corporations Act*.[2] Both *Acts* state directors must "exercise the care, diligence and skill that a reasonably prudent person would exercise in comparable circumstances."

To enhance awareness among boards of the need to protect clients' privacy, the Information and Privacy Commissioner/Ontario (the IPC) has prepared this paper for dissemination to directors. The purpose of this paper is to raise awareness of privacy not only as a compliance issue but also as a business issue. In doing so, we hope to promote the understanding that oversight of an organization's privacy compliance policies and procedures is an integral and necessary component of effective board service.

A lack of attention to privacy can have a number of adverse consequences for which directors may be held accountable. The degree of risk will vary from one organization to the next, depending on the nature of the business and the amount of personal information that is collected, used and disclosed. The potential consequences include:

- damage to the organization's reputation and brand;
- physical, psychological and economic harm to customers whose personal information is used or disclosed inappropriately;
- financial losses associated with deterioration in the quality and integrity of personal information due to customer mistrust;
- loss of market share or a drop in stock prices following a "privacy hit" resulting in negative publicity or the failure or delay in the implementation of a new product or service due to privacy concerns.

1 R.S.O. 1990, c. B.16
2 R.S.C. 1985, c. C-44

Careful attention to privacy issues may not only help directors and their organizations to avoid these risks, but may also have a number of positive effects. The potential benefits of implementing sound privacy policies and practices include:

- consumer confidence and trust;
- a more positive organizational image and a significant edge over the competition;
- business development through expansion into jurisdictions requiring clear privacy standards;
- enhanced data quality and integrity, fostering better customer service and more strategic business decision-making;
- enhanced customer trust and loyalty; and
- savings in terms of time and money.

The remainder of the paper is divided into six sections. The first section describes what is meant by a "culture of privacy." The second describes the challenges of publicized data breaches. The third describes basic fair information practices – the foundation for privacy. The fourth section describes the potential risks that directors and officers take when they fail to pay close enough attention to privacy in their organizations. The fifth describes some of the potential benefits that can be reaped through the implementation of sound privacy policies and practices. The final section sets out recommendations for what directors should do to promote privacy compliance in their organizations. The paper concludes with a list of questions directors should ask senior management about the privacy policies and practices in their organizations to ensure privacy compliance.

Culture of privacy

Increasingly, privacy is one of the key issues on which directors must focus in order to execute their compliance and managerial oversight as well as mitigate risk. Privacy is often defined as the right of individuals to control the collection, use and disclosure of their own personal information (i.e., information that relates to an identifiable individual). Organizations can help to protect an individual's privacy by implementing what are commonly referred to as fair information practices as part of an overall culture of privacy. Such a culture moves beyond legislation, regulation and policy to help ensure that errors do not occur. It also provides the necessary imperative to promptly detect and correct errors if they do occur. Thorough training, ongoing monitoring, auditing, and regular evaluation are key components of a culture of privacy.

Telling your executive team to "Make us privacy compliant" is not enough.[3] Directors must be more engaged, approve their company's privacy plan, and require regular report backs. It is also important to treat privacy as a business issue and not as a compliance issue. If you make privacy part of your business strategy, then it will be infused in your work plan and your staff will come on board fully. However, if you treat it solely as a compliance issue, then you will be doing the minimum necessary, and seldom advancing privacy as you would if you viewed it as a strategic business differentiator.

3 See, for example, Thomas J. Smedinghoff, "Director Responsibilities for Data Security: Key Questions the Board Should Ask," *Directors Monthly* (April 2007).

Learning from privacy breaches

New information technology, the globalization of the economy, the interconnectivity of businesses, and web-based delivery of products and services pose challenges to the protection of personal information. These challenges are reflected in a number of well-publicized privacy breaches.

In a truly regrettable incident, a patient admitted to an Ontario hospital made a specific request to ensure her estranged husband, who worked at that hospital, and his girlfriend, a nurse at the hospital, did not become aware of her hospitalization, and that steps be taken to protect her privacy. The patient later learned that the nurse had repeatedly and surreptitiously accessed her electronic health record both before and after she filed a privacy complaint with the hospital's privacy office. Although her file was flagged with a privacy warning for those seeking access, the nurse was still able to see the patient's file by clicking "yes" to a "Do you wish to continue?" prompt. Following the hospital's report on this incident, the patient filed a complaint with the IPC, which resulted in an order requiring the hospital to overhaul its privacy practices.[4]

Further examples of repeated breaches include those at TJ Maxx and the Canadian Imperial Bank of Commerce (CIBC). The TJ Maxx breach began in July 2005 when one or more intruders stole 45.7 million customer credit and debit card numbers. Data was stolen repeatedly from 2005 to 2007.[5] CIBC experienced a repeated breach from 2001 to 2004 when misdirected faxes with confidential customer information were sent to a West Virginia scrap yard despite repeated calls from the owner to have the faxes stopped.[6] And in January 2007, CIBC's subsidiary Talvest Mutual Funds lost 470,000 pieces of customer account information.[7]

Since incidents such as these can have serious consequences for both the individuals whose privacy is breached and the organization that is responsible for the breach, questions have been raised about the liability risks of directors in protecting the personal information collected, used and disclosed by their organizations. For example, criminal charges were laid against Hewlett-Packard's Chair of the Board following surveillance of several board members, which included access to their telephone records.

4 *Order HO-002* (July 27, 2006), Information and Privacy Commissioner/Ontario Decision: **http://www.ipc.on.ca/images/Findings/up-HO_002.pdf**.

5 Joseph Pereira, "Breaking the Code: How Credit-Card Data Went Out Wireless Door," *The Wall Street Journal* (4 May 2007).

6 *Addendum to CIBC fax incident summary: Summary of Investigations* (April 18, 2005), Office of the Privacy Commissioner of Canada: **http://www.privcom.gc.ca/incidents/2005/050418_02_e.asp**.

7 "CIBC loses data on 470,000 Talvest fund customers," *Canadian Broadcasting Corporation* (January 18, 2007), CBC: **http://www.cbc.ca/money/story/2007/01/18/cibc.html**.

Most Canadian organizations are required to comply with either federal or provincial privacy legislation. In addition, those conducting business in the U.S. must ensure compliance with data breach notification laws first passed by California in 2002 and currently in force in most states.[8] Legislation and the potential risk of harm from privacy breaches are not, however, the only factors compelling directors to pay closer attention to privacy issues. Research shows that consumers are becoming increasingly concerned, better informed and more demanding with regards to the protection of their personal information. Studies show that consumer trust translates into customer retention, a competitive advantage, and a willingness to pay more if customers know that their privacy will be protected.[9] The opposite is also true.

Surveys show that consumers will alter their purchasing behaviour, adversely for the interests of the business involved, if they no longer trust an organization to manage their personal information appropriately. According to 2006 statistics data loss can translate into an eight per cent loss of customers and a corresponding decrease of eight per cent in revenue, plus $100 in expenses per customer for notification and restoring data.[10]

8 See, for example, the National Conference of State Legislatures page on data breach notification laws: **http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm**.

9 See, for example: IT Policy Compliance Group, "Taking Action to Protect Sensitive Data: Benchmark Research Report" (February 2007); Ponemon Institute, LLC, "Privacy Trust Survey for Online Banking" (April 5, 2005). See also coverage of the 2007 TriCipher Consumer Online Banking Study conducted by Javelin Strategy & Research: "Consumers Value ID Theft Prevention Over Financial Reimbursement," *Insurance Journal* (April 10, 2007): **http://www.insurancejournal.com/news/national/2007/04/10/78595.htm**; "Fear Of Identity Theft Discourages Consumers From Banking Online" *Bank Systems & Technology* (May 8, 2007): **http://www.banktech.com**. In addition, see Don Peppers and Martha Rogers, Ph.D., *Return on Customer: Creating Maximum Value From Your Scarcest Resource*, (Random House Inc., 2005) Chapter 12, "Violate your customer's trust and kiss your asset good-bye."

10 IT Policy Compliance Group, "Taking Action to Protect Sensitive Data: Benchmark Research Report" (February 2007).

What are Fair Information Practices?

Fair information practices are a set of common standards that balance an individual's right to privacy with the organization's legitimate need to collect, use and disclose personal information. In Canada, fair information practices are set out in the Canadian Standards Association Model Code for the Protection of Personal Information (the CSA Code). The CSA Code is incorporated into federal private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act*. As of January 1, 2004, all private sector organizations in Canada that collect, use or disclose personal information during the course of commercial activity have been subject to the federal legislation, except in jurisdictions that have substantially similar provincial legislation such as Alberta, British Columbia and Quebec. Ontario's *Personal Health Information Protection Act* is also designated as substantially similar under the *Personal Information Protection and Electronic Documents Act*.

The CSA Code consists of 10 principles. First, it requires the designation of at least one individual who is accountable for the organization's compliance with the other nine principles (**Accountability**). The organization must specify the purposes for which it collects personal information, at or before the time when the information is collected (**Identifying Purposes**). The consent of the individual must be obtained for the collection, use or disclosure of personal information, except where it is not appropriate to obtain consent (**Consent**). The collection of personal information must be limited to that which is necessary to fulfil the specified purposes (**Limiting Collection**). Personal information must not be used or disclosed for purposes other than those for which it was collected, unless the individual consents or as required by law (**Limiting Use, Disclosure, and Retention**). Personal information must be as accurate, complete and up-to-date as necessary for the purposes for which it is to be used (**Accuracy**). The organization must implement security safeguards that are appropriate for the level of sensitivity of the personal information (**Safeguards**). The organization must make readily available specific information about its policies and practices relating to the management of personal information (**Openness**). Individuals have a right to access and request correction of their own personal information (**Individual Access**). Finally, individuals must be able to challenge an organization's compliance with the privacy principles (**Challenging Compliance**).

A single Global Privacy Standard (GPS) was developed last year after my office, and a Working Group of Commissioners I chaired, harmonized leading privacy practices and codes from around the world. The final version of the GPS was formally tabled and accepted in 2006 at the 28th International Data Protection Commissioners Conference, in the United Kingdom. The GPS builds upon the strengths of existing codes containing time-honoured privacy

principles and, for the first time, reflects a noteworthy enhancement by explicitly recognizing the concept of "data minimization" under the collection limitation principle.[11]

Directors should be familiar with the Generally Accepted Privacy Principles (GAPP) developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants.[12] GAPP is based on fair information practices, and specifically details the management component, which says that an organization must define, document, communicate, and assign accountability for its privacy policies and procedures.

Directors would be proactive in satisfying their duties by assessing whether senior management has successfully implemented these practices in their organizations. A list of questions based on these principles that a director might ask is presented at the end of this document. It should be noted that the limitations placed on the collection, use and disclosure of personal information will, in many cases, require modification to existing information management practices.

11 See *Creation of a Global Privacy Standard*, by Commissioner Ann Cavoukian, Ph.D., Information and Privacy Commission/Ontario: **http://www.ipc.on.ca/images/Resources/up-gps.pdf**.
12 *Generally Accepted Privacy Principles*, American Institute of Certified Public Accountants: **http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/**.

What are the Potential Risks of Failing to Address Privacy?

1. A privacy breach could be damaging to you and your organization's reputation and business relationships

A significant privacy breach could lead to unwanted publicity and additional scrutiny of you and your organization. Even in cases where media attention can be avoided, a formal complaint to the Privacy Commissioner could result in adverse information about your organization becoming public. This could lead to further unwanted scrutiny by both privacy and consumer advocates.

Directors have a duty to act with the standard of care that a reasonably prudent person would exercise in similar circumstances. Directors can look to the federal privacy legislation for guidance on the standard of care that organizations should adhere to in protecting personal information. Companies and their directors may be sued for negligence if they have failed to conform to the required standard of care in their actions or inactions.

In addition, the U.S. federal Trade Commission has looked to the following practices, as a whole, to determine that a company failed to provide reasonable and appropriate security for sensitive customer information:[13]

- created unnecessary risks to sensitive information by storing it in multiple files when it no longer had a business need to keep the information;
- failed to use readily available security measures to limit access to its computer networks through wireless access points on the networks;
- stored the information in unencrypted files that could be easily accessed using a commonly known user ID and password;
- failed to limit sufficiently the ability of computers on one in-store network to connect to computers on other in-store and corporate networks; and
- failed to employ sufficient measures to detect unauthorized access.

Since adverse publicity arising from privacy breaches could have an impact on stock prices, shareholders may question whether the directors of an organization have conformed to the standard of care in acting or failing to act – this could lead to shareholder-initiated lawsuits.

13 *DSW Inc.* F.T.C. File No. 052 3096 (March 7, 2006). See also *BJ's Wholesale Club, Inc.,* F.T.C. File No. 0423160 (September 20, 2005).

The interconnectivity of businesses adds an additional layer of risk. Where businesses are working collaboratively on partnering and joint initiatives, privacy should be a major consideration. Businesses that have made a commitment to privacy protection will not want to expose themselves to risk through associations or partnerships with organizations that fail to conform to the required standard of care in protecting personal information. The Wall Street Journal reported in May 2007 that following the TJ Maxx breach "banks could spend $300 million to replace cards from just one year's worth of stolen numbers," and that the breach could total $20 million in fraudulent transactions.[14] Questions are being raised about whether a regulatory response should require businesses to reimburse banks for costs they incur from a business' data breach.[15]

Directors will want to ensure that privacy is a key consideration when their organizations enter into partnership arrangements, or when contractual arrangements are made with companies for the provision of specific services (e.g., information technology). An organization cannot avoid their privacy obligations by outsourcing to third parties, and may be held liable if agents and service providers fail to comply with privacy legislation. Conversely, to avoid lawsuits initiated by business partners, organizations should take reasonable steps to meet the minimum requirements for privacy protection set out in all contractual agreements with third parties and in privacy legislation.

In addition, to help minimize the damage following a privacy breach, directors should ensure that their organizations have a privacy crisis management protocol in place. The protocol should ensure that, following a privacy breach, appropriate steps are taken to minimize the damage to you and your organization's reputation and business relationships and to prevent similar breaches in the future. As part of the protocol, directors should be kept informed about all privacy breaches.

2. A privacy breach could result in serious harm to your customers

Directors need not only be concerned about the potential threat of lawsuits initiated by shareholders and business partners following a privacy incident. A privacy breach could also potentially expose you, your organization and your business partners to lawsuits initiated by customers who are the victims of a privacy breach.

Launching class-action lawsuits stemming from privacy breaches has emerged as a new litigation trend. In many situations, companies that have inadvertently used or disclosed

14 Joseph Pereira, "Breaking the Code: How Credit-Card Data Went Out Wireless Door," *The Wall Street Journal* (4 May 2007).

15 For example, the TJ Maxx breach triggered the introduction of a bill this year in the company's home state of Massachusetts. See H.B. 213, "An Act Relative to Enhancing the Confidentiality and Protection of Certain Customer Information," 185th Gen. Court, Reg. Sess., Mass., 2007.

the personal information of individuals without their consent have subsequently been sued. For example, the legal fallout from TJ Maxx's loss of 45.7 million customer credit and debit card numbers includes challenges from customers, shareholders – and banks wanting reimbursement for the cost of replacing cards.[16] The potential for serious harm is recognized by the U.S. Federal Trade Commission which has found that it is an unfair practice to fail to secure customers' sensitive information because it can cause substantial injury that a consumer cannot reasonably avoid.[17]

Individuals may suffer a range of harms from the unauthorized or inappropriate collection, use and disclosure of their personal information. One of the more widespread harms is the unwanted intrusion into our lives from junk mail, spam and telemarketing. But, individuals can also be exposed to more serious risks including physical, psychological and economic harm. Unauthorized disclosures of seemingly innocuous personal information, such as address and telephone number, can expose some individuals, including children, to the risk of physical harm from stalkers, abusive partners, or sexual predators.

Individuals can be humiliated or stigmatized through the disclosure of personal information relating to medical or psychiatric conditions, alcohol or drug addiction, or financial status. Unauthorized disclosures of certain types of personal information to some third parties can lead to a loss of opportunities in terms of employment, insurance, housing, and other benefits and services. Furthermore, if an organization does not take appropriate steps to guard against it, personal information that is inaccurate, incomplete or out-of-date could be used to make administrative decisions that adversely affect individuals. For example, inaccurate financial information could be used to deny an individual access to credit.

Identity theft is another growing risk that needs to be addressed. If your organization fails to implement adequate privacy and security safeguards, this may open the door to identity thieves who attempt to gain access to enough personal information to assume the identity of another person, usually for the purpose of committing crimes in that person's name. Identity thieves may go on spending sprees, take over bank accounts, open new accounts, divert financial mail, rent apartments, and apply for loans, credit cards, utilities and social benefits – all at the expense of their victims! Victims of identity thieves are often left without any credit, their reputations in ruins and may even be arrested for the crimes of the persons who impersonated them. With a poor credit rating, a victim may be denied a job, a loan, or rental housing.[18]

16 Bill Brenner, "Banks prepare lawsuit over TJX data breach," *Security Search* (25 April 2007): **http://searchsecurity.techtarget.com**.

17 Federal Trade Commission, News Release/Communiqué, "BJ'S Wholesale Club Settles FTC Charges" (16 June 2005): **http://www.ftc.gov/opa/2005/06/bjswholesale.shtm**.

18 See, for example, the Canadian Internet Policy and Public Interest Clinic's *Identity Theft: Introduction and Background* Working Paper No. 1 (ID Theft Series): **http://www.cippic.ca/en/bulletin/Introduction.pdf**.

The Solicitor General reports that identity theft is one of the fastest growing crimes in Canada, with Canadian credit bureaus receiving from 1,400 to 1,800 identity theft complaints each month.[19] In 2006, the PhoneBusters National Call Centre received 7,778 identity theft complaints from Canadians, with total losses in excess of $16 million.[20]

Even where there is no intent, it could be argued that liability for financial and other losses may be attracted, if you and your organization do not take reasonable steps to mitigate this known threat. At a minimum, these steps should include the implementation of security measures that are appropriate to the level of sensitivity of the personal information being protected. Also, in the event that there is a privacy breach, your privacy crisis management protocol should require notification of individuals whose privacy has been breached so that they may take appropriate steps to protect themselves from harmful consequences, such as identity theft. View relevant resources on the IPC's website (**www.ipc.on.ca**), including our *Identity Theft Revisited: Security is Not Enough*, *What to do if a privacy breach occurs: Guidelines for government organizations*, and *Breach Notification Assessment Tool,* co-written with British Columbia's Information and Privacy Commissioner.

Thus, from a risk management perspective, it is very important that directors be aware of whether their organization is being proactive in taking steps to prevent breaches from occurring – well before they arise – and to minimize the damage caused by any breaches that do occur, in spite of your organization's best efforts at prevention.

3. A lack of attention to privacy could lead to customer mistrust and deterioration in the overall quality of your organization's information assets

In today's information economy, the quality and integrity of information is critical to the success of most businesses. Accurate, complete and up-to-date information is required to provide products and services designed to meet the needs of individuals and to make informed business decisions. The best way to ensure customer data accuracy is by collecting data from the customer directly, with their knowledge and consent, as well as by allowing customers easy access to their personal information. "The 1:1 enterprise, operating in an interactive environment, relies not just on information *about* customers, but information *from* them," says Don Peppers and Martha Rogers, Ph.D., in their book, *Enterprise One to One: Tools for*

19 Canada, *Public Advisory: Special Report for Consumers on Identity Theft*, (Ottawa: Department of the Solicitor General of Canada and the United States Department of Justice, 2002): **http://ww2.ps-sp.gc.ca/publications/policing/Identity_Theft_Consumers_e.asp**.

20 "Statistics on Phone Fraud: Identity Theft Complaints," PhoneBusters: **http://www.phonebusters.com/english/statistics_E06.html**.

Competing in the Interactive Age.[21] Personal information has greater value when it is closer to the customer, and that value is enhanced with the use of consent, according to Peppers and Rogers in their book *Return on Customer*.[22] In a 2007 study, the Ponemon Institute identified consumer consent as one of the five essential ingredients to building consumer trust.[23]

A loss of data integrity and quality will have a direct impact on your organization's ability to make sound business decisions and to provide your customers with the types of products and services that they need. Without accurate data, an organization will have no way of knowing who its customers are and how they behave. This could result in financial losses for which directors may be held accountable.

Research shows that almost all companies admit that inaccurate customer data is costing them money in terms of ineffective marketing strategies and damage to their brand and reputation. In spite of this, a large proportion of organizations do not have policies and procedures to enhance the accuracy of their customer data.

Fair information practices require that personal information be as accurate, complete and up-to-date as necessary for the purpose for which it is to be used. Adhering to this accuracy principle can have a direct impact on the quality and integrity of your information assets. In addition, implementing fair information practices can have an indirect benefit by influencing your customers' attitudes and behaviour. If customers do not feel that an organization can be trusted to handle their personal information properly, they may do a number of things: they may avoid providing complete information, withhold consent for the use and disclosure of their personal information, or worse – provide misleading or inaccurate information.

For example, research has shown that the vast majority of Internet users are concerned that the personal information they provide online will be used in an unauthorized way. As a result of this lack of trust, users rarely provide accurate personal information online. About 70 per cent of users report that they will typically abandon a website that requests personal information and about 40 per cent report having entered false information to gain access to a site.[24]

In short, the implementation of fair information practices can help you and your organization to enhance customer trust and avoid the financial losses associated with a lack of data quality

21 Don Peppers and Martha Rogers, Ph.D., *Enterprise One to One: Tools for Competing in the Interactive Age* (New York, NY: Random House, 1999).

22 Don Peppers and Martha Rogers, Ph.D., *Return on Customer: Creating Maximum Value From Your Scarcest Resource*, (Random House Inc., 2005).

23 Charles Giordano of Bell Canada, "Use privacy to build customer trust, loyalty," *DM News* (23 March 2007).

24 Graphic, Visualization, & Usability Center, "7th WWW User Survey" (1997): **http://www.gvu.gatech.edu/user_surveys/survey-1997-04**. See also, Joann Loviglio, "Online news registration may not deliver," *USA Today* (13 June 2004): **http://www.usatoday.com/tech/webguide/internetlife/2004-06-13-news-site-reg_x.htm**.

and integrity. You must respect customer consent and their right to access their personal information, and everyone in your company must respect it. That respect must be reflected in all your practices, in the way you build your databases – everywhere! It can never be an afterthought.

4. A lack of attention to privacy could result in a loss of market share, additional costs, and a drop in stock prices

There are a number of other ways in which a lack of attention to privacy may affect your organization's profits and stock prices. Customers who lack trust in an organization may decide to take their business to a competitor with stronger privacy practices. Mistrust and a corresponding loss of business could be the result of a failure to implement a privacy policy, the implementation of an ineffective privacy policy, specific breaches of your customers' privacy, or privacy-related incidents that attract adverse publicity. According to a an online banking study released in 2007, 41 per cent or 88 million customers would change banks or reduce service usage with a bank that suffered a data breach, providing further indication that protecting privacy is very competitive business.[25] Thus, it is becoming increasingly clear that the cost of mismanaging privacy can have ramifications that go far beyond legal liability. Privacy policies are not worth the paper they are printed on if you do not build a culture of privacy within your organization. Privacy must be incorporated into your daily practices. Train your staff, and then tell your customers what you are doing to protect their privacy.

Business could also be lost if an organization attempts to introduce a product or service without carefully considering its impact on privacy. On some occasions, consumer backlash has forced companies to abandon plans to implement new products and services that were seen to be privacy invasive. This could happen after substantial investments have been made in the development and promotion of a product or service. For example, public outrage forced two companies to abandon the rollout of a product that would have provided the personal information of 120 million American consumers on a compact disk. In the first few months following the announcement of this product, there were over 30,000 consumer inquiries and complaints. Other companies have been forced to abandon plans to embed their products with radio frequency identification tags (RFIDs) when an influential consumer group called for a consumer boycott over privacy issues inherent in what it referred to as a "smart shelf" spy system.[26]

25 TriCipher, "Consumer Online Banking Study" (March 2007).

26 For example, in 2003, Italian clothier Benetton sparked a furor after it announced plans to implant RFID tags in its apparel; in 2004, retailer Metro AG began issuing loyalty cards with RFID chips embedded and did not tell consumers, which triggered a worldwide boycott; and also in 2004, Verichip raised ethical and religious issues with its sub-dermal RFID implants and registration services.

Delays in the rollout of a product or service to permit privacy issues to be addressed after the fact can also be costly. For example, in one incident, a manufacturer of computer chips was forced to redesign its latest computer chip when the plan to embed a unique identification number prompted two prominent privacy groups to call for a consumer boycott of all of the manufacturer's products. Delays such as these could leave the door open for a competitor to capture greater market share. In addition, it is often far more expensive to retrofit a product or service to enhance privacy than to build in privacy protections up-front, at the design stage.

Directors who ensure that privacy is part of their organization's culture can minimize the risk of financial losses resulting from a loss of business due to customer mistrust, cancellation or delays in the rollout of new products or services that are seen as impinging on privacy rights, and retrofitting products or services in accordance with privacy legislation and customer expectations. Directors can also minimize the chance of additional costs which flow from a data breach, such as the cost to investigate and contain the breach, notification to customers, and legal costs. The TJ Maxx breach could cost, excluding lawsuit liabilities, more than $1 billion in five years according to the Wall Street Journal.[27]

27 Joseph Pereira, "Breaking the Code: How Credit-Card Data Went Out Wireless Door," *The Wall Street Journal* (4 May 2007).

What is the Business Case for Sound Privacy Practices?

1. Sound privacy practices will give your organization a more positive image and a significant edge over the competition

In today's highly competitive marketplace, most businesses rely heavily on brand image to differentiate their product or service from those of their competitors. Considerable resources are invested in advertising, communication, and general branding of a product or service. Negative publicity about one or more privacy breaches or poor privacy practices in general can do irreparable damage to a business's hard-earned brand image. The implementation of sound privacy policies and practices can be thought of as a kind of insurance for an organization's investment in its brand and image.

Privacy has become a business imperative emerging from the public's increased awareness of the value of their personal information. Where there are gaps in the privacy practices of competitors, privacy-sensitive consumers will choose to do business with those organizations that can demonstrate a clearer commitment to privacy and security. Thus, sound privacy practices will protect and enhance your organization's image and brand, as well as its bottom line.

2. Adherence to fair information practices can facilitate business development through expansion into other jurisdictions with privacy laws

Directors should be aware that privacy is a global issue. The original impetus for privacy legislation in Canada was the introduction of the European Union (EU) Directive on Data Protection, which prohibits the flow of personal information to countries where there are inadequate levels of privacy protection. To ensure the unimpeded free exchange of personal information across international borders, many countries have introduced privacy laws, or are in process of doing so.

In an interconnected and global business environment, weak privacy and security safeguards can impose a non-economic trade barrier to organizations that want to conduct business in jurisdictions with higher privacy standards. Awareness of international standards will help directors determine whether their organization's business practices will permit expansion into international markets.

3. Sound privacy policies and practices will allow you to customize your products and services to meet customer needs and will enhance strategic decisions

Directors should understand that customer information, lawfully collected by your organization, is a valuable asset – one that can be a useful tool in building relationships with customers. An organization's best source of information is its customers themselves. As one 2007 study noted, customers are willing to help you with protecting their privacy. It found consumers will readily take extra measures if the solutions provided by the company are simple and convenient.[28]

As noted previously, the integrity and quality of the personal information that your organization collects from its customers will depend on the extent to which your customers trust your information management practices. If your customers are confident that your organization will use their personal information properly, they will be more likely to share personal information that is accurate, complete and up-to-date. This will allow your organization to provide products and services that are tailored to your customers' preferences and to make sound business decisions based on the knowledge of who your customers are and how they behave.

In today's highly volatile and competitive marketplace, consumers are demanding more tailored offers for products and services, more convenience and better customer service. The Canadian Marketing Association estimated that every year direct marketing generates more than $51 billion in the sale of goods and services. To meet the challenges of today's business environment, organizations must know their customers intimately. Openness and transparency in information management practices and sound privacy policies provide a foundation upon which relationships with customers can be built and sustained.

4. Sound privacy policies and practices will enhance customer loyalty

As consumers are beginning to demonstrate a growing recognition of the value of their personal information and the importance of its security, the need for organizations to address privacy has become more pressing. Surveys consistently show that consumers will change their purchasing behaviour if they no longer trust an organization to manage their personal information. Whether the lack of trust stems from a publicized privacy breach or an individual's personal experience with your organization, the damage to your bottom line may be irreparable.

28 TriCipher, News Release/Communiqué, "Study Shows Banks Could Increase Profitability By $8.3 Billion Per Year If Stronger Security Measures Implemented," (21 March 2007): "When asked if they would download identity protection software from their financial institution, 62%, or 102 million, consumers said that they would be likely to do so. Consumers' willingness to download security software to protect financial information was further confirmed when 69% of respondents, or 113 million consumers, reported having downloaded some form of security software in the last six months."

Frederick Reichheld in his book, Loyalty Rules!, has shown that an increase in customer retention rates of five per cent increases profits by from 25 to 95 per cent. This is largely due to the low cost of retaining existing customers in comparison to the high cost of acquiring new customers through advertising and special promotions. Sound privacy policies and practices are one component of a good customer retention strategy.

5. A proactive approach to privacy will save you time and money

There are many ways in which a proactive approach to privacy can save you and your organization time and money. For example, you could save time and money by avoiding the following:

- lawsuits initiated by customers, shareholders and business partners;
- inquiries and complaints from your customers;
- an investigation or audit by the Privacy Commissioner;
- inefficiencies resulting from poor information management practices and the retention of inaccurate, incomplete or outdated information;
- failure of a new product or service that is seen as impinging on privacy rights;
- delays in the rollout of a new product or service in order to address privacy concerns; and
- retrofitting of a product or service to address privacy concerns after it has been designed and implemented.

It is clear that the investment that your organization makes in preventing privacy breaches today could save you time and money spent on damage control for years to come.

What Should Directors Do?

1. Education is key – directors should ensure that they receive appropriate training in privacy and that there is some privacy expertise on their board

Directors should ensure that their knowledge about best privacy practices is current and up-to-date. Depending on the needs of the organization and those of the board, there are a variety of approaches that can be taken for educating directors. For example, the board could invite privacy experts to speak at one or more of their meetings; organize a privacy workshop for directors and senior officers of their organizations; or attend one of the many privacy workshops organized by third parties.

In addition, where it is feasible, boards should establish a committee whose terms of reference include privacy. The membership of this committee should develop a degree of expertise in privacy and should be familiar with the nature and scope of the personal information collected by the organization. In order to ensure that the interests of management do not overshadow the need for sound privacy practices, it is vital that outside directors are represented on this committee. Ideally, an outside director should chair the committee, as this will help to enhance its independence from management.

2. Directors should ensure that at least one senior manager has been designated to be accountable for the organization's privacy compliance

Accountability is a key fair information practice. Organizations can demonstrate accountability through the appointment of a member of senior management whose responsibilities include privacy or whose primary responsibility is privacy. In many organizations, this individual is known as the Chief Privacy Officer (CPO).

The CPO (or equivalent) is the organization's resident privacy expert. He or she must be given the authority to oversee the design, implementation, monitoring and reporting on the organization's privacy policies and to ensure that the company's privacy compliance system and control measures comply with existing legislation. This individual should be responsible for ensuring the harmonization of privacy practices on an enterprise-wide basis. Depending upon the size and the scope of the business, the role of the CPO will vary. However, regardless of the size of the organization, the CPO has a crucial role to play – this individual must be knowledgeable about all aspects of the business.

Directors should ensure that the person appointed to carry out the functions of the CPO maintains a certain degree of separation from other senior managers of the organization. Independence will facilitate oversight of the organization's privacy policies and practices.

3. *Directors should ensure that privacy compliance is a part of senior management performance evaluation and compensation*

The designation of one or more individuals to oversee privacy compliance is not sufficient to ensure that privacy is being appropriately addressed throughout the organization. Before privacy policies and procedure can be effective, all senior managers have to make a commitment to privacy protection. Privacy compliance should be one of the criteria upon which senior managers are evaluated and compensated.

4. *Directors should ask senior managers to undertake periodic privacy self-assessments and privacy audits and to report to the board on these activities on a regular basis*

A good way to ensure ongoing privacy compliance is through regular self-assessments and privacy audits. A useful self-assessment tool is the Privacy Impact Assessment (PIA). The PIA is a systematic assessment tool designed to assess the impact of an application of new information technology or the introduction of new products and services. The PIA allows privacy issues to be identified and addressed throughout the design and implementation of a new technology, product or service. All innovations or modifications to existing information systems or products and services should undergo a PIA. Since the PIA can serve as an early warning system and risk assessment tool, directors should ensure that they receive and review all PIA reports.

Privacy audits are another useful tool that can be conducted by the CPO (or equivalent) or by external privacy consultants. From an oversight perspective, it is preferable for the audit to be conducted by someone who is independent from the organization. The purpose of the audit is to ensure that the organization is in compliance with its own privacy policy and with existing legislation. The goal of the audit should be to promote education and awareness and to find practical solutions to everyday privacy issues. Audits should be conducted at regularly scheduled intervals, such as annually. As is the case with PIA reports, directors should ensure that they receive and review reports on all privacy audits.

In *Return on Customer*, authors Peppers and Rodgers recommend telephoning your own call center several times to assess the company's privacy compliance:

> Ask what options you have to manage the process. Tell someone you have a complaint about how your own privacy was violated, and ask to speak with someone about it – then see whom they connect you to. Ask if your name or personal details

have ever been given to any other firm, and whether that firm will be bound by the same privacy protection principles.[29]

5. Directors should ensure that they ask senior management the right questions about privacy practices in their organization

Keeping in mind the interests of shareholders and other stakeholders, including the company's employees and customers, directors have a responsibility to ensure the appropriate level of managerial oversight of privacy.

The duty of care that directors owe to their organizations entails that directors must ask the right questions of management – questions that will give management the opportunity to demonstrate compliance with both legislation and best privacy practices and generate "bottom-line" advantages that result from implementing sound privacy policies. Below is a list of questions that directors may wish to ask to ensure privacy compliance.

29 Don Peppers and Martha Rogers, Ph.D., *Return on Customer: Creating Maximum Value From Your Scarcest Resource*, (Random House Inc., 2005) at 182.

Questions Directors Should Ask to Ensure Privacy Compliance

1. Has your organization designated at least one individual to be responsible for privacy?

2. Does your organization collect personal information? If so, would any of this information be considered to be sensitive?

3. Is the purpose for the collection of personal information explained to customers at the time it is collected?

4. Is personal information collected only for purposes that are appropriate in the circumstances?

5. Is the personal information that is collected, used or disclosed by your organization limited to that which is necessary to achieve the specified purpose?

6. Have all necessary consents been obtained for the collection, use or disclosure of personal information?

7. Is the form of consent appropriate for the level of sensitivity of the information and consistent with the reasonable expectations of the individual?

8. Have controls been implemented to ensure that personal information is as accurate, complete and up-to-date as necessary for the purpose for which it is to be used?

9. Are the security safeguards to protect personal information appropriate for the level of sensitivity of the information?

10. Are the information management practices of the organization transparent? Does the organization make available to customers information about its policies and practices relating to the handling of personal information?

11. Do customers have the right to access and correct their own personal information?

12. Is there a mechanism through which customers can make an inquiry or complain about the organization's personal information management practices?

13. Has an organizational privacy policy been implemented? Is the privacy policy available to the public?

14. Has an employee privacy policy been implemented?

15. Has a privacy crisis management protocol been implemented to deal with privacy breaches? In the event of a privacy breach, do you communicate information to individuals whose privacy has been breached so that they may take appropriate steps to protect themselves from harmful consequences, such as identity theft?

16. Are all employees aware of the organization's privacy policy? Is privacy training, tailored to roles and responsibilities, mandatory for all employees?

17. Are privacy requirements built into contractual agreements with business partners and service suppliers and agents?

18. Are privacy requirements built into all employment contracts? Do these contracts include consequences for breaching the organization's privacy policy?

19. Does your organization conduct a privacy impact assessment prior to implementing new technologies, programs, products or services that could impact on privacy?

20. Does your organization have a compliance program that includes regular privacy self-assessments and privacy audits to ensure compliance with your privacy policy and privacy legislation?

Information and Privacy Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
CANADA

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca