Privacy Exposures and Risk Reduction Strategies for Small Organizations

October 2013

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner
Ontario, Canada

Eduard Goodman, J.D., LL.M.
CIPP-US/C
Chief Privacy Officer
IDT911™

Acknowledgements

The authors wish to acknowledge the contribution of Michelle Chibba, Director, Policy and Special Projects, and Fred Carter, Senior Policy & Technology Advisor at the Information and Privacy Commissioner's Office, to the development of this paper. We also wish to acknowledge the assistance of the IDT911 editorial staff, senior management, and ownership who actively support international consumer awareness and business education on fraud prevention, privacy, and data risk management best practices.

Information and Privacy Commissioner
Ontario, Canada

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
Privacy by Design: www.privacybydesign.ca

Privacy Exposures and Risk Reduction Strategies for Small Organizations

TABLE OF CONTENTS

Introduction

In the past decade there has been a sea change in the information management practices of organizations of all sizes. As firms' operations become more networked and data-intensive, personal information and customer trust have become critical assets that must be managed accordingly. Small organizations everywhere recognize that privacy is good for business but often lack the resources and expertise needed to effectively minimize privacy-related risks. Growing transparency and breach notification requirements provide additional incentives to firms to strengthen their governance, risk management and compliance practices and to become more accountable to customers, regulators, business partners, and shareholders. In spite of these growing expectations and requirements, it often takes a data breach incident to deliver the message that poor privacy is indeed bad for business. Regrettably, "Privacy by Disaster" is an unfortunate way to learn this lesson; for small enterprises, the consequences of failing to prevent and mitigate risk are potentially fatal.

A much better way forward is to proactively adopt *Privacy by Design* (*PbD*). Unanimously approved in 2010 by international privacy and data protection authorities as an international standard, *Privacy by Design* represents the evolution of fair information practices and a significant raising of the bar for privacy measures. *PbD* principles aspire to the highest global standard of privacy protection. They emphasize active prevention of breaches, systematic and verifiable methods of risk management, and achieving privacy protection goals through innovative, optimal techniques that also satisfy non-privacy objectives. The 7 Foundational Principles of *Privacy by Design* are as follows[1]:

1. ***Proactive*** not Reactive; ***Preventive*** not Remedial
2. Privacy as the ***Default Setting***
3. Privacy ***Embedded*** into Design
4. Full Functionality – ***Positive-Sum,*** not Zero-Sum
5. End-to-End Security – ***Full Lifecycle Protection***
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***
7. ***Respect*** for User Privacy – Keep it ***User-Centric***

The data privacy environment is shifting for small businesses in Canada. Technology now allows companies of nearly any size to gather, manage, and share huge amounts of private information about customers, clients, and patients. This has put smaller organizations on equal footing with large businesses in terms of their attractiveness to criminals interested in obtaining this sensitive information to commit fraud. However, small businesses frequently don't have the staffing or financial wherewithal to devote significant resources to data protection efforts, a fact that sometimes makes them particularly appealing to criminal fraud rings and identity thieves. Understanding where privacy exposures often originate and the

1 See Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Revised 2011)

best practices that can help to prevent them are part of the portfolio of tools small organizations can use to protect themselves from the dangers of data breaches.

The ultimate aim of *Privacy by Design*'s proactive approach is to mitigate the risk of privacy harms from arising in the first place, ideally preventing them entirely, whilst preserving a commitment to functionality. *Privacy by Design* principles go further to prescribe systematic methods to detect breaches early and respond effectively with appropriate containment and remediation techniques. More than ever, a holistic approach is required. From the perspective of small enterprises, the challenge is to operationalize these *PbD* principles with limited expertise and resources. This paper summarizes our guidance and options for reducing privacy exposures and risk in small organizations.

How do data exposures happen?

Ontario was the first jurisdiction in Canada with mandatory breach notification requirements since the passage of the 2004 *Personal Health Information Protection Act* (*PHIPA*). The Office of the Information and Privacy Commissioner of Ontario (IPC) receives hundreds of breach notices each year, many from small, private health-care practitioners. The IPC also receives voluntary breach reports from across the entire public sector, under both the *Freedom of Information and Privacy Protection Act* (*FIPPA*) and the *Municipal Freedom of Information and Privacy Protection Act* (*MFIPPA*). This gives the IPC a unique perspective on current information security trends in Ontario, and allows the office to play a constructive role early in the breach remediation processes.[2]

Organizations, large and small, public and private, face three main kinds of data breaches today: physical, logical, and procedural.

- *Physical failures* involve the loss of control over a physical asset containing personal information. This type of failure is comprised of documents, portable data storage media such as flash drives or tapes, and computer hardware that have been lost or stolen.
- *Logical failures* involve intentional access to information without access to the physical asset, either unauthorized access by an insider or the exploitation of vulnerability by an outside hacker.
- *Procedural failures* result from data custodians mishandling personal information, exposing it to unauthorized parties. These failures include the unintentional exposure of information on a website, exposure in mailings, misdirected faxes, mailings and email, and improper disposal or abandonment of information or media.[3]

2 See IPC annual reports for statistics, and *A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight* (2009)

3 For a good discussion, see C. Matthew Curtin, CISSP, and Lee T. Ayres, CISSP, "Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry," 4 ISJLP 525–922 (2008), 569-601. See also Office of the Alberta Information and Privacy Commissioner Breach Report (2013), at www.oipc.ab.ca/Content_Files/Files/Publications/Causes_of_Breaches_June_2012.pdf

Opportunities for data security issues arise from other areas, as well. The potential pitfalls that come along with vendor relationships, for example, affect nearly every small enterprise in Canada. The majority of small and mid-sized firms rely to some degree on support organizations, from payroll service providers to HR consultants to marketing professionals. In addition, many small businesses are vendors to larger companies. In order to successfully operate, many of these relationships require that sensitive data be transferred, stored, and managed. When a small enterprise uses a vendor, it must work to ensure that all privacy issues are overseen as part of the work agreement. Any lapse in best practices by the vendor will almost certainly reflect badly on their client—everything from reputation damage for exposure of the private information to potential civil liability for the event. And in those instances where a small organization itself is the vendor, it may be unknowingly taking on the larger organization's risk without putting appropriate measures in place to ensure that data privacy is managed in a way that protects both client and vendor.

The IPC has carried out investigations, provided guidance, and issued Orders related to all three types of breaches, some of which could have been easily prevented. By all accounts, the incidence of data breaches is growing along with their visibility and impacts to the organization and affected individuals.[4] Whether regulated by us or not, organizations of all sizes today are expected to understand evolving vulnerabilities and threats to their information assets, have in place appropriate technological, policy/administrative and legal/contractual controls to mitigate identified privacy risks, and be prepared to respond quickly with a coherent and effective response plan when —not if— the inevitable breach occurs.

Special considerations for small enterprises

Small organizations may be at higher risk for data exposures based on a number of special considerations. Any enterprise that accepts payment cards or is involved in processing payment card data, whether it's within the brick-and-mortar retail sector or a Web-based business, is at significant risk of a security breach exposing private payment card information. Companies that have contractual relationships with other firms—for example, the agreements that exist between franchisors and their franchisees—may find themselves in a gray area when it comes to determining who is responsible for controlling and protecting the private customer and payment card data that the two groups may exchange. Professional service firms are also likely to have additional data privacy concerns. Physicians and other health-care providers must carefully manage the large amounts of personal health data entrusted to them and even have sector specific obligations in Ontario under the *Personal Health Information Protection Act* (*PHIPA*). Attorneys and law firms hold information that may be valuable to criminals who are intent on gaining access to private and company information. Insurance brokers, accountants, and payroll providers must often share personal financial data that could be devastating to consumers if exposed. In short, any small company that relies on sensitive information must give close consideration to how it protects that information.

4 See Cavoukian & Tapscott, Privacy and the Open Networked Enterprise (2006)

How serious is the issue of a privacy breach for small businesses? Quite simply, an exposure could be an extinction-level event for a company that is unprepared to manage it. Customers are often hesitant to do business with an organization that doesn't adequately protect its data, and the damage to a firm's reputation could dissuade enough customers to the point that the company is no longer sustainable. The financial impacts of a breach can also be calamitous. A small business without the resources to pay for legal assistance, forensic investigations, the required notifications, remediation measures, and the fines, penalties, or judgments that could arise in the event of a privacy breach event, just might find itself out of business.

Risk reduction strategies

Small businesses in Canada have a number of approaches available to them as part of an overall data breach risk reduction strategy. Privacy policies and procedures alone, without a concrete strategy for implementation, will not protect an organization from privacy risks. This section outlines seven steps that organizations should consider implementing in order to effectively translate their privacy policies into privacy practices, and to mitigate privacy risks to residual levels.

1. **Implement a privacy policy that reflects the privacy needs and risks of the organization and consider conducting an effective Privacy Impact Assessment.**

Each organization, regardless of its size, should develop and implement an overarching privacy and security policy that applies to all aspects of its information management processes (i.e., the collection, use, retention, disclosure, and destruction of personal information). This policy should be consistent with industry standards, as well as any Orders, guidelines, fact sheets, and best practices issued by the IPC.[5]

For organizations holding sensitive personal information or large amounts of personal information, we recommend that a comprehensive Privacy Impact Assessment (PIA) of the organization's data holdings and processes be undertaken. PIAs and other risk assessment tools (such as a security threat assessment) can assist in determining the vulnerabilities that exist within an organization, thereby enabling it to develop and implement a privacy policy that addresses a broad range of issues.[6]

5 See IPC Fact Sheets, Best Practices and Professional Guidelines, *inter alia*

6 See IPC *Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default* (2010) and *A Pragmatic Approach to Privacy Risk Optimization: Privacy by Design for Business Practices* (2009); and P. Jeselon & A. Fineberg, *A Foundational Framework for a PbD-PIA* (2011)

2. Link each requirement within the policy to a concrete, actionable item, such as operational processes, controls and/or procedures, in effect translating each policy item into a specific practice that must be executed.

While having a strong privacy policy is important, it is only the first step. An organization, and more specifically senior management, needs to develop and implement a method of translating the policy into a series of specific practices or action items that must be executed within the organization's operations. For every requirement set out in the policy, the organization should consider how it can most effectively achieve it through concrete, actionable items. These actionable items must clearly identify who is responsible for executing them and how each requirement will be met.[7]

3. Demonstrate how each practice item will actually be implemented.

In order to effectively implement change within an organization, there needs to be strong "buy in" from the top. Senior management needs to be aware, not only of the organization's privacy policy, but also how that policy is going to be operationalized through concrete actionable items.[8]

4. Develop and conduct privacy education and awareness training programs to ensure that all employees understand the policies/practices required, as well as the obligations they impose.

Employees need to understand data privacy and how to manage sensitive information. While privacy awareness and training will help to achieve end-to-end security – an important *PbD* principle – it is also key to enabling a broader, proactive organizational approach to privacy. Proper training enables employees to internalize privacy protection goals and create a heightened awareness of potential privacy issues. All employees (including the senior management team, departmental managers, and frontline staff) should attend an initial privacy orientation as well as regular continuing privacy training. Where feasible, we also recommend that organizations develop privacy education/training procedures that identify the timeframe, frequency, and content of both the initial orientation and ongoing privacy training, to ensure that training remains formalized and standardized within the organization. Different awareness methods and educational tools should be utilized, depending on context and needs.[9]

5. Designate a central "go to" person for privacy-related queries within the organization.

Even the best employee training will not answer all privacy-related challenges that an organization may face in its day-to-day operations. Consequently, every organization should have a central "go to" person (or group) who can answer internal questions about privacy requirements or the implications of particular practices on privacy. In smaller organizations, it may not always be practical to create an employment position that is devoted solely to managing privacy concerns

7 See IPC *Privacy Diagnostic Tool Workbook* (2005), *Identity Theft Revisited: Security is Not Enough* (2005), and *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* (2012)

8 See IPC *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices* (2009); and *Privacy and Boards of Directors: What You Don't Know Can Hurt You* (2007).

9 See IPC *A Policy is Not Enough: It Must be Reflected in Concrete Practices* (2012)

within the organization. However, there still needs to be a "go to" person who is knowledgeable and responsible for privacy-related issues.[10]

6. Verify both employee and organizational execution of privacy policies and operational processes and procedures.

Beyond education and training, organizations must ensure that policies are made actionable. There must also be processes and procedures in place to verify that employees are complying with the organization's privacy policies. There are various methods, both formal and informal, that organizations can and should be using to verify compliance. One should never assume that policies are being met – trust, but verify.[11]

7. Proactively prepare for a potential privacy breach by establishing a data breach protocol to effectively manage a breach

It is increasingly important that organizations of all sizes be prepared to react to data security incidents, such as a privacy breach. A privacy breach occurs when personal information is collected, retained, used, or disclosed in ways that are not authorized. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information.

When a privacy breach or suspected breach occurs, it is imperative that the organization react both quickly and effectively to manage the situation. As a result, we strongly advocate that organizations develop and implement protocols to address the identification, reporting, containment, notification, investigation, and remediation of privacy breaches. All employees need to know what to do and who to notify in the event of a privacy breach (or suspected privacy breach). The organization also should have rules that address when and how senior management will be notified. The organization also should strongly consider contacting the Information and Privacy Commissioner's office at an early stage so that staff can provide guidance and assistance in responding to the breach.[12]

Cost-shifting strategies and insurance

Small organizations should strongly consider some of the cost-shifting strategies available to them in case all their "best laid plans" are laid to waste and they still suffer some form of privacy breach event. Canadian enterprises of all types and sizes have a growing variety of insurance options available to them as the final step in a strategy to defend against and respond to data privacy breaches. This insurance should not be looked at as the solution, but more like the caboose on the privacy breach prevention-and-response-planning train. And with the ever growing options of insurance solutions available, there are several varieties and types of policies that are available to help defray the financial and reputational impact of a data privacy exposure.

10 See IPC *Privacy by Design: From Policy to Practice* (2011)

11 See IPC *Manual For The Review and Approval Of Prescribed Persons And Prescribed Entities* (April 2012)

12 See IPC *Breach Notification Assessment Tool* (2006); *Privacy Breach Protocol Guidelines for Government Organizations* (Rev 2012); and *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector* (Rev 2012)

While these insurance polices are often generally referred to as “cyber” coverage, most small organizations are really more focused on what is more accurately termed data privacy breach coverage. This coverage typically consists of two main types of coverage: First party coverage is the most common, based on small business needs and risks. Third party (liability) coverage often is available as an add-on coverage.

First party coverage explained

One facet of a comprehensive privacy breach prevention and response plan is first party insurance coverage. This type of policy helps companies cover expenses related to managing the breach itself. Those costs may include notifying affected parties and engaging investigative services, such as forensic and diagnostic expertise, to determine the type and cause of the breach. The expenses that result from a data privacy breach may be impacted not only by the scope and nature of the breach, but also by notification, call handling for customer inquiries, remediation for impacted consumers, and other measures to help protect those individuals potentially impacted by a small businesses privacy breach event. Effectively managing the crisis of a breach through first party coverage could determine how much money a small enterprise ultimately pays out-of-pocket for the exposure, and whether or not they even survive the event financially.

Third party coverage explained

Third party coverage also is a vital element to include in any risk mitigation plan. This is a policy that provides coverage for costs a business may incur related to liability claims, the need to mount a legal defense or respond to lawsuits and the obligation to pay judgments, settlements, fines, or penalties levied as a result of a data exposure. The scope of these financial impacts can vary widely, and may be influenced by the complexity of the breach, the timeliness and effectiveness of any actions taken by the business when the exposure was discovered, governmental regulations of punitive fines, and jury decisions in the case of litigation.

It is important to remember that coverage solutions add to a company’s power to respond to a potential exposure, rather than taking away from its duty to protect the information to begin with. Developing and judiciously following a robust proactive plan is crucial to success and is usually a condition for the insurance policy to even cover the event.

Conclusion

Small organizations are being squeezed, on the one hand, by evolving threats to personal information assets and, on the other, by heightened transparency and accountability requirements for managing those assets. With limited resources and expertise devoted to privacy and security issues, data breaches represent potentially extinction-level events.

The costs of responding to a breach can be enormous, but working to prevent breaches and planning for privacy risk are cost-effective investments. Applying the basic concepts of *Privacy by Design* in a small enterprise setting is essential to avoid the pitfalls of unnecessary or unauthorized data processing. *PbD* supports developing better organizational awareness of fundamental best practices when collecting, using, and disclosing sensitive personal, information. But small organizations should also look at their specific industry and area of operations to help them measure their privacy breach risks and potential sources of exposure. Fortunately, many useful resources and tools exist to help them. Once a plan to mitigate, identify, and respond to a breach has been developed, regular review of that plan will allow the enterprise to adapt to the evolving threat landscape and any changes in regulatory requirements, best practices, and its business plan or scope.

The *Privacy by Design* framework requires a holistic, integrative and systematic approach to managing privacy and security risks throughout the entire personal data lifecycle. Small organizations that follow the guidance set out in this paper can achieve higher operating efficiencies while minimizing risks and costs to optimal levels.

IPC References

- Privacy and the Open Networked Enterprise (2006)
- A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight (2009)
- Fact Sheet #12: Encrypting Personal Health Information on Mobile Devices (May 2007)
- Fact Sheet #16: Health-Care Requirement for Strong Encryption (July 2010)
- Fact Sheet #18 - Secure Transfer of Personal Health Information (August 2012)
- Encryption by Default and Circles of Trust: Strategies to Secure Personal Information in High-Availability Environments | Press Release (2012)
- Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default (2010)
- A Pragmatic Approach to Privacy Risk Optimization: Privacy by Design for Business Practices (2009)
- "A Foundational Framework for a PbD-PIA" by P. Jeselon and A. Fineberg (2011)
- Privacy Diagnostic Tool (PDT) Workbook (2005)
- Identity Theft Revisited: Security is Not Enough (2005)
- Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices | Press Release (2012)
- Privacy by Design: Essential for Organizational Accountability and Strong Business Practices (2009)
- Privacy and Boards of Directors: What You Don't Know Can Hurt You (2007)
- A Policy is Not Enough: It Must be Reflected in Concrete Practices (2012)
- Manual For The Review and Approval Of Prescribed Persons And Prescribed Entities (2012)
- Privacy by Design: From Policy to Practice (2011)
- Breach Notification Assessment Tool (2006)
- Privacy Breach Protocol Guidelines for Government Organizations (Revised 2012)
- What to do When Faced With a Privacy Breach: Guidelines for the Health Sector (Revised 2012)
- Privacy and Security by Design: A Convergence of Paradigms | Press Release (2013)

External Resources

- Canadian Institute of Chartered Accountants: Privacy Resources
- SANS Institute: Twenty Critical Security Controls for Effective Cyber Defense
- Office of the Privacy Commissioner, Canada:

  - Privacy Guide for Small Businesses: The Basics
  - Privacy Questionnaire: Is Your Business Ready?
  - Securing Personal Information: A Self-Assessment Tool for Organizations

- Office of the Information and Privacy Commissioner, Alberta

  - Guide for Businesses and Organizations on the Personal Information Protection Act
  - Ten Steps to Implement PIPA
  - Getting Accountability Right with a Privacy Management Program

- Office of the Information and Privacy Commissioner, British Columbia

  - A Guide for Business and Organizations to BC's Personal Information Protection Act

- Nicholas F. Cheung, Claudiu S. Popa, The Canadian Privacy and Data Security Toolkit for Small and Medium Enterprises

Overview of the Organizations

Information and Privacy Commissioner of Ontario, Canada (IPC)

The role of the Information and Privacy Commissioner of Ontario, Canada, is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The IPC acts independently of government to uphold and promote open government and the protection of personal privacy. Under the three *Acts*, the Information and Privacy Commissioner: resolves access to information appeals and complaints when government or health-care practitioners and organizations refuse to grant requests for access or correction; investigates complaints with respect to personal information held by government or health-care practitioners and organizations; conducts research into access and privacy issues; comments on proposed government legislation and programs; and educates the public about Ontario's access and privacy laws. More at: www.ipc.on.ca and www.privacybydesign.ca.

IDT911™

Founded in 2003, IDT911 is North America's premier consultative provider of identity and data risk management, resolution and education services. The company serves over 17.5 million households across North America and provides fraud solutions for a range of organizations, including Fortune 500 companies, North America's largest insurance companies, corporate benefit providers, banks and credit unions and membership organizations. Since 2005, the company has helped more than 600,000 businesses manage their risk of data breaches. IDT911 is the proud recipient of several awards, including the Stevie Award for Sales and Customer Service and the Parent Tested, Parent Approved award for social networking monitoring tool SocialScout. For more information, please visit www.idt911.ca, www.facebook.com/idt911 and www.twitter.com/idt911.

Office of the Information and Privacy Commissioner, Ontario, Canada
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: 416-326-3333
Fax: 416-325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

IDT911 Services | IDT911, Inc.
1080 Beaver Hall, Suite 700
Montreal, QC H2Z 1S8
514.360.3700 main
514.360.3701 fax
Website: www.idt911.ca

Web site: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

October 2013

Information and Privacy Commissioner, Ontario, Canada

IDT911